Department of Home Affairs

Canberra, Australian Capital Territory

13 April, 2023

RE: 2023-2030 Australian Cyber Security Strategy Discussion paper

My name is Dr Cassandra Cross and I am an Associate Professor in the School of Justice, Faculty of Creative Industries, Education and Social Justice, at the Queensland University of Technology. I am a leading internationally recognised scholar in the field of fraud, financial crime, and cybercrime. I first started researching fraud fifteen years ago in 2008, while working as a civilian with the Queensland Police Service. In 2011, I was awarded a Churchill Fellowship to explore the prevention and support of online fraud victims. This enabled me to travel across the UK, US, and Canada to engage with over 30 agencies working in this space. It was an invaluable experience which was the catalyst to my academic transition.

My appointment to QUT in September 2012 has enabled me to pursue a research agenda focused heavily on fraud. I have developed an extensive and authoritative track record in this area, across both national and international fronts. I have published over 90 outputs predominantly relating to fraud and cybercrime. This includes co-authoring the monograph *Cyber Frauds, Scams and their Victims* (published by Routledge in 2017). I have been successful in bidding for, and attracting research funding, having led eight research projects, all in collaboration with government or industry partners, totaling over AUD$1.8 million.

My research has focused on all aspects of fraud victimisation, across policing, prevention, disruption, and the support of victims. A large amount of my research has involved interviewing fraud victims and gaining their direct narratives of what occurred and the aftermath of the incident. I have spoken with hundreds of victims, as well as a large array of professionals (including law enforcement, consumer protection, government, industry, banking and finance, victim support) on this issue across the globe. My focus has also extended into examining identity crime and data breaches, both of which are relevant to the current submission.

Fraud and cybercrime are global issues, and my work has highlighted the complexities, nuances, and ongoing challenges posed to individuals, governments, corporates, and society as a whole.

I thank the Department of Home Affairs for their consideration of this submission.

Dr Cassandra Cross
Associate Professor, School of Justice, Faculty of Creative Industries, Education and Social Justice, Queensland University of Technology

[redacted]

The following submission addresses three questions from the discussion paper that relate directly to my research expertise.

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

It is vital that any revised strategy take into account victim perspectives, both at an individual and organization level. Cybercrime impacts millions of Australians each year, and there is a formal need to acknowledge this in the Cybersecurity Strategy. The 2016 strategy omitted victims entirely from its content, while the 2020 strategy made limited references to victims in relation to the promotion and funding of iDcare (Australia and New Zealand's identity crime support centre) to deliver assistance to Australians affected by identity crime. Based on my research, one of the biggest needs cited by fraud victims (which extends to those affected by data breaches and identity crimes) is the desire to be heard and acknowledged. It is important that the Cybersecurity strategy does this. Further, it is important that any acknowledgement to victims of cybercrime is done in a constructive manner, and one that does not ascribe blame or perpetuate the negative stereotypes of greed, gullibility and culpability, that many current victims will experience. While some victims are arguably active in their victimisation (though under high levels of coercion and deception) a large number of individuals find themselves affected through no fault of their own. This is particularly the case with the recent large-scale data breaches of Optus, Medibank and Latitude. The targeting of Australians by global cyber offenders is a sad but inevitable outcome, and while the strategy should take this into account, it should also create a framework and vision for concrete measures of prevention, disruption, and support to be implemented by relevant agencies.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

The reporting of cybercrime incidents is a challenging area for many victims. The known levels of cybercrime victimisation are likely to be severely underestimated. In a 2013 report, the United Nations estimated that only 1% of all cybercrime was reported to authorities. In this way there is a substantial discrepancy between what we know and what is actually occurring.

There are many known barriers to the reporting of these incidents. These include (but are not limited to) not knowing who to report to, a belief that nothing can be done, the shame and embarrassment about being victimized, and the cross-jurisdictional nature of most cybercrime offences. Of those who do report, many experience overwhelming negativity at the hands of the justice system, and do not receive an outcome that meets their expectations. Further, victims often encounter what is termed the "merry-go-round effect", where they are passed from one agency to another in their attempts to lodge a complaint or get a response to their incident.

The creation of ReportCyber (and formerly ACORN), is a positive step to addressing some of the concerns expressed by victims in their attempts to lodge a complaint. Having a central point of reporting for all cybercrime incidents is beneficial in this way. However, there are still a number of associated challenges that this does not address. The requirement of victims to lodge a complaint for a cybercrime incident to an online reporting portal is distressing for some victims. I have spoken with many who have attempted to lodge a complaint with police agencies in person, but who have been turned away and told to report online. Having been traumatized through online communication methods, the requirement to lodge a complaint through this same technology can be difficult for some. Cyber incidents often reduce the level of trust in online platforms, which should be acknowledged. In this way, an alternative should be provided for those who need it.

Second, any online form can provide variable quality and quantity of data. Without human screening and direction, victims will provide what they believe to be the most important aspect of their circumstance. This may not always be relevant or have investigative value. Further, many victims may be unaware of the realities of their circumstance, and what has actually happened. The use of lies and deception is high, as well as a lack of technical knowledge on some of the complexities and sophistication evident in some cybercrime events. In this way, strong and clear guidance should be provided to any online, central reporting mechanism.

Third, there is a disconnect between the expectations of lodging a complaint. This partially stems from some victims having unrealistic understandings of the nature of their incident and the prevalence of cybercrime victimisation across the country. Lodging a complaint online, with an automatic response leaves many feeling underwhelmed and frustrated at a perceived lack of care and priority.

Despite ReportCyber being the central reporting mechanism for cybercrime offences, there are still a range of other reporting avenues available to victims. This includes Scamwatch, the eSafety Commissioner, and banks/financial institutions to name a few. This could be further exacerbated with the proposed establishment of a National Anti-Scams Centre by the Federal government. Currently there is no clear differentiation across the many reporting avenues that exist, and victims are likely to attempt to report to all portals in the hope that this will increase the likelihood that they receive a response to their complaint.

Overall, a single reporting mechanism has clear advantages, but in its current state, it is still lost within the broader ecosystem, and this can impact negatively on victims (both individual and organizational) who are attempting to lodge a complaint and receive a response. Any proposed changes to this should seek to reduce, rather than increase, the potential for these identified issues to either continue or escalate.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Effective prevention is an ongoing challenge. One of the main issues revolves around an inability for individuals to connect with their potential for victimisation. Nobody intends to be a victim, but it is an outcome for many. In some cases, this is through an action or

behaviour they have engaged in, intentionally or otherwise. In many cases, victims are aware of best practice, but in the moment or based on the circumstances, have not carried this out. For others, it is a result of a third-party incident, as is evident in the ongoing reporting of data breaches. In this way, it is difficult to promote an effective prevention message to a person who doesn't have control over their information. The best individual cyber security practices will not guard against third party incidents.

In this way, it is important to promote the collective benefits of general cyber security practices (strong passwords, updated software etc.) however the recent data breaches have clearly shown a need for society more broadly to have a robust conversation about the amount of data requested and collected by agencies, and the length of time it is stored. Continually placing the onus on individuals to protect themselves is redundant in the context of organisational breaches. A shared responsibility is needed on all sides.

In terms of support for victims, victims desire to be heard and to be acknowledged. They should be treated respectfully regardless of their circumstances. Cybercrime affects each individual differently, and support needs will therefore vary. There are limited support services available in Australia to assist victims of cybercrime. iDcare is the exception to this, who provide high quality, individually tailored support to a small proportion of overall victims.

In part, the lack of support services stems from the shame and stigma associated with particular types of victimisation and the aforementioned negative stereotype that places responsibility on the victims themselves for what has happened. There is a critical need to provide greater support for cybercrime victims. This is needed up front in the form of recognition of what has occurred and an assessment of the extent of the harm (both financial and non-financial aspects of victimisation) incurred. This would then dictate what support is needed. Support may be practical (helping to secure a device or removing malware) or health related (providing counselling to assist with levels of depression or physical decline). Research indicates that the impacts of cybercrime can be significant on victims' health and wellbeing and can have ongoing consequences. There can also be levels of fear and anxiety that exist with the uncertainty of what has occurred, or what might occur into the future, particularly relevant to identity crime and data breaches.

It is unlikely that police agencies are the most appropriate agency to provide support. Therefore, there is potential for industry to provide relevant support services, centering victim needs and prioritizing victim recovery.

Overall, a revised cyber security strategy provides an opportunity to better acknowledge victims of cybercrime and provide both a vision and framework that government and industry can use to reduce the harm and prevalence of cybercrime, as well as provide better outcomes to those who experience cybercrime victimisation.

For a copy of all my publications (which I have drawn upon in this submission), please see the following link:

https://eprints.qut.edu.au/view/person/Cross,_Cassandra.html