22 August 2017

Enquiry into the circumstances in which Australians’ Medicare information has been made available on the ‘dark web’ – Submission by the Centre for Internet Safety

The Centre for Internet Safety is pleased to provide this submission. The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cyber crime and threats to cyber security.

This Enquiry has the opportunity to explore the various aspects of trust, safety and confidence interacting for consumers engaging with government in the online environment. For too long this important component of cyber security has not been addressed, with emphasis always being placed on introducing technical measures as a means to providing such security around government service delivery.

With respect to the terms of reference:

Any failures in security and data protection which allowed this breach to occur

The Centre is not aware of any technical failure in this area within the Department. However, due to the lack of meaningful communication arising from the Department or relevant Minister, it is unknown how such a breach of Medicare numbers actually occurred. The Centre is of the belief this compromise of data was by an ‘end user’ who had bone fide access to the Medicare system, but who was abusing this access for financial gain.

Should this be the case, then there has been a major policy and procedural failure by the Department with monitoring, investigating and prosecuting unlawful access by legitimate users.

The implications of this breach for the roll out of the opt-out My Health Record system

The move, more than two years ago, from the Personally Controlled Electronic Health Record (an opt in system) to the My Health Record (an opt out system) has done little to quell public anxiety surrounding the placement of sensitive health details into the online world. The accompanying communication strategy has not been compelling to the public, especially surrounding the security aspects.

Cyber security has now become a mainstream topic of conversation from the boardroom to the kitchen table. The rate of media reporting on cyber breaches of government agencies, companies and citizens is unprecedented. This will only rise over time as we spend more time online in social settings, work environments or accessing government services. Australian’s are early and eager adopters of the internet and associated technologies, however the constant reporting of breaches is diminishing their trust, safety and confidence. On the current path, less and less people will trust the government with their health details.

- How our digital footprints are collected and managed by the organisations (including government) we have relationships with will have long term implications.
- The promotion of privacy issues and the importance of the protection of personal information is critical to ongoing functioning of the online environment.
- Government technology projects, including My Health Record, should create 'benefit profiles' to measure the extent of consumer trust, safety and confidence in the intended service delivery.

The Department needs to ask itself the following questions.

Does the customer:

- Know what data is being collected?
- Know what the data will be used for?
- Know who will have access to it?
- Give consent - informed consent - for it's collection?
- Have the ability to opt out of such data collection and still be able to use the service?

Until the Department adequately addresses the trust, safety and confidence benefits of the My Health Record and competently communicates this to the public then uptake will be very slow.

The response to this incident from government – both ministerial and departmental

As discussed earlier, the response to the public from both the Department and the Minister was disappointing. The messaging was confusing and often contemptible. Unfortunately we are plagued by a culture at all levels of government to 'spin' the message, including events related to cyber security. There is nothing good to come from this in the long term.

Considered use of language to clearly communicate cyber security issues is critical, particularly in response to cyber incidents. Effectively communicating cyber security concepts can build confidence, provide assurance and convey opportunity. It can be the difference in whether management of a cyber incident, such as the one being investigated by the Committee, is perceived as a success or failure.

Until we reach a maturity where Departmental and Ministerial spokespersons are fully educated on cyber terminology; the broader online threat environment and its impact on public trust, safety and confidence; combined with a willingness to accept mistakes and inform citizens how they are being addressed then we will never move forward with full adoption of the My Health Record (and indeed many other government online service delivery projects).

Nigel Phair
Managing Director