dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

hello@dspanz.org
dspanz.org

8 April 2022

Department of Home Affairs

Via email: Ransomware.Action@homeaffairs.gov.au.

Re: Proposed Ransomware Incident Reporting Obligation

To Whom it May Concern:

DSPANZ welcomes the opportunity to make this submission on behalf of our members and the business software industry.

While we support the objectives underpinning the proposed Ransomware Reporting obligation, DSPANZ is concerned about adding an extra reporting obligation for Australian businesses without a clear corresponding benefit. Many Digital Service Providers (DSPs) are already required to report this information to the ATO under the Operational Security Framework in addition to other reporting obligations e.g. the Notifiable Data Breach Scheme. Many other businesses would be in a similar situation.

Please find our comments on the *Proposed Ransomware Incident Reporting Obligation Fact Sheet* below.

Why Ransomware?
There is no clear definition for ransomware included in the factsheet. Ransomware is often broadly defined which makes it confusing for businesses to understand when they are required to report. Without having examples of what businesses are and are not required to report, the ACSC can expect to see businesses reporting a range of their security incidents as they look to do the right thing.

Who will be required to report?
Applying the reporting obligation to businesses with annual revenues of over $10 million will capture many small businesses who may not have the security expertise to understand what the obligation involves. For this reason, the whole reporting process should be kept simple and unambiguous, yet informative, to assist those with little technical or security knowledge.

What will need to be reported?
The proposed 12 hour reporting window seems too short for a private business reporting scheme unless Home Affairs is planning to create a notification mechanism to warn other businesses about reported incidents. A 12 hour window is

particularly challenging when a cyber event occurs overnight or outside business working hours e.g. on a weekend.

The Operational Security Framework, which many DSPs are required to meet, asks DSPs to report immediately from the time a DSP is made aware of an incident but recognises that within 72 hours is acceptable where the incident has been contained within the DSP's environment.

For these reasons, DSPANZ recommends adopting the standard 72 hour notification window as it will be less disruptive and allow businesses to provide better intelligence about the incident. This will result in higher quality data being submitted to the Australian Cyber Security Centre (ACSC). However, we do recognise that it is good practice to report incidents as soon as possible.

We are interested in discussing the reporting window further with Home Affairs and ACSC to allow for a better understanding of the issues that smaller and non-technical businesses will face if there is a 12 hour reporting window.

Further clarification is required on what constitutes both a significant impact and a relevant impact and what is meant by "materially disrupted" to ensure there is an understanding across all business sizes. The guidance for each of these terms will need to be clear especially to help those businesses without security expertise. We also recommend providing detailed examples of scenarios where there is a significant impact on a business and then a relevant impact on a business.

We would like a clearer statement about what information and evidence will be required at both notification levels. It may be difficult for smaller or non-technical businesses to understand their obligations and provide the appropriate information.

What is also unclear is what the consequences may be for businesses who do not report.

How to make a report?

For those businesses that are already required to report security incidents to a regulator or government agency, like DSPs under the Operational Security Framework, there should be an option to report to one body (e.g. the ATO) and have them notify other government agencies or departments as appropriate. This would be much more efficient than requiring businesses to notify multiple agencies about the one security incident.

DSPANZ would appreciate the opportunity to engage further on this submission. For further information, please contact Maggie Leese.

About DSPANZ

Digital Service Providers Australia New Zealand is the gateway for the government into the dynamic, world class business software sector in Australia and New Zealand. Our members range from large, well-established companies through to new and nimble innovators who are working at the cutting edge of business software and app development on both sides of the Tasman.

Yours faithfully,

Simon Foster
President & Director
DSPANZ