dspanz. digital service providers australia new zealand

SSAM Review Session 2 - Meeting Summary & Outcomes

Agenda Item	Description
1	**Welcome and Acknowledgment of Country** Matthew Prouse welcomed attendees to the session and acknowledged the Traditional Owners.
2	**ATO visibility of apps across the DSP ecosystem** Diana Porter shared the following statistics on the app ecosystem: ● 150 apps integrating with multiple DSPs ● 30% increase in app market growth ● 23 DSP products have reported marketplaces Diana also shared that the ATO have received 44 security incident reports from DSPs in FY 2020-21. It is unclear how many of these 44 reports came from the third party ecosystem. This led to wanting to explore the breach reporting requirements for add-ons later in the session.
3	**Recap of Session 1** Simon Foster provided a recap of the first review session. The group accepted that this was an accurate summary of the previous session.
4	**Review of Survey Feedback So Far** Matthew Prouse ran through preliminary insights of both the add-on and DSP SSAM review surveys. It was noted that we still haven't achieved the goal of the SSAM - for add-ons to complete a security review that can be accepted by all DSPs. Instead, we have a consistent set of standards being applied by DSPs with marketplaces. DSPANZ will produce a report on the SSAM survey and it will be presented as part of Webinar Week in October.
5	**Breach Reporting for Add-ons** Simon Foster outlined a previous experience of providing a breach report to DSPs. While it was an unsuccessful breach, Simon still went to report it and found that no one wanted to know the details and because add-ons don't have a direct relationship with the DPO, he couldn't report it to them either. This raised the question of whether add-ons should be reporting the same information multiple times or should they report to one DSP and expect them to share this information. Another breach experience was shared with the group where they described how it can be difficult to tell whether a breach is real or not and this, accompanied with tight reporting timelines, may mean there isn't enough time to determine how serious a breach is. It was noted that the OAIC Notifiable Data Breach scheme couldn't be leveraged as

	this covers personal information only and currently excludes small businesses. The ATO are also not able to share information back without it being anonymised, meaning that it could not be actioned by DSPs or add-ons. Thought needs to be given to how this system would work to make this process easier for both DSPs and add-ons.
6	**Rollout & Implementation Experiences** Xero shared their experience implementing and rolling out the SSAM for their add-on ecosystem. While they use SecurityScorecard, they noted that it still requires people to manually review answers from add-ons. They raised that if changes are made to the SSAM, that DSPs will need time for internal change management. AccountKit then shared their experience implementing it as an add-on. They noted that SecurityScorecard was valuable alongside other measures. It was questioned how DSPs would check against any added operational controls.
7	**Meeting Summary** Matthew Prouse summarised the session into the following points: ● Number one problem is that there are a lot of different questionnaires ● DSPs have broadly standardised their requirements for marketplaces but not their wording or documentation. What do we need to do so that DSPs can trust the certificates of their competitors? ● Implementation of SSAM is positive but it is asking a small number of people to do the work to uplift their security **Next Steps and Action Items** Consider the following questions before the next session: ● What do you constitute as a security incident? Are they reportable? ● How do you want breaches shared so that it saves time? The next session will focus on the overlap of SSAM with other security standards and controls that may be in scope for the SSAM. Please review the alternate controls in scope for the SSAM review document before the next session.