



Key Outcomes

UNCLASSIFIED External

Title:	Focus Group - Security sharing and awareness key outcomes		
Issue date:	6 February 2019		
Event date:	9 January 2019	Start: 14:00	Finish: 15:00
Chair:	Jim Meyer	Facilitator:	Kylie Johnston
Contact	Sonya Summers	Contact phone:	02 472 57383
Attendees: names/section	DSP: Aaron OConnor (XERO) Brian Miller (Intuit) David Field (Ozedi) Dennis Lee (MYOB) Ian Gibson (SuperChoice) John Marzella (MYOB) Michael Wright (Sage) Mike Denniss (Class) Rob Cameron (FYI software) Robert Fabian (Advance Payroll)	ATO: Christian Motuzas (ATO) Elijah Kusa (ATO) Gary Read (ATO) James Meyer (ATO) Kylie Johnston (ATO) Megan Gosche (ATO) Simon Kert (ATO) Sonya Summers (ATO)	
Apologies	Dennis Lee (MYOB), Marius Nel (MYOB), Ann White (Ozedi), Chris Howard (ADP/ABSIA), Paul MacPherson (Xero)		
Next meeting	Proposed		

Information Sharing and Awareness – General Discussion

James Meyer opened discussions around whether DSPs are interested in leveraging the security information the ATO is able to share.

The ATO advised they would share information from discussions with the Australian Cyber Security Centre (ACSC).

MISP¹ was mentioned as a possible solution for managing Cyber Threat Intelligence (CTI).

The ATO has MISP integrated with detection tools, and uses it as a central repository for technical information which has been compromised.

Many DSPs utilise data centres (Managed Service Providers) to host their services. Managed Service Providers (MSP) generally provide automated CTI feeds. There was general uncertainty around whether DSPs could share the information held by their MSP.

Action item:	Due date:	Responsibility:
20190109-01	Next meeting	DSPs
The ATO is seeking feedback on <i>Cyber Security Posture of MSPs (see attached)</i> to determine its usefulness in supporting DSP security posture.		

It was suggested DSPs consider establishing a relationship with ACSC as they may be able to provide a centralised source for CTI once further established.

The group discussed the challenges associated with tracking threats when IP addresses continually change.

Some expressed concerns with sharing CTI as it might provide a competitive advantage.

The group agreed there was a need for an industry standard for intelligence gathering, monitoring and sharing, and it should be at a much higher level (eg: MSP or national).

Next Steps:

- Meetings will be facilitated monthly
- ATO will discuss a case study to generate further conversation around sharing of CTI moving forward

¹ MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing, <https://www.misp-project.org/>