Topic: Australian Sanctions Office - Ransomware

Senator Helen Polley

Question

The committee heard there is no substantive guidance available from the Australian Sanctions Office about the reasonable precautions and due diligence required of a company making a ransomware payment in order to satisfy the defence under current sanctions legislation (Committee Hansard [Proof], 23 May 2024, pp. 2–3).

• Could you please provide some background to these legislative provisions and their rationale?
• What guidance is the Australian Sanctions Office able to provide regarding the type of conduct that would satisfy the defence?

Answer

The Government's focus is on pursuing and deterring perpetrators of ransomware attacks and the sanctions were directed towards that end. The explanatory statements (https://www.legislation.gov.au/F2024L00522/asmade/downloads) for the designation of individuals under Australia's autonomous thematic cyber sanctions framework state the rationale for these legislative measures as follows:

> Autonomous sanctions are measures not involving the use of armed force which the Australian Government imposes as a matter of foreign policy in response to situations of international concern. Such situations include significant cybercrime incidents and malicious cyber activity threatening Australians and Australian government entities.
>
> Autonomous thematic cyber sanctions demonstrate Australia's commitment to deterring and responding robustly to malicious and significant cyber incidents. The imposition of sanctions also signals to persons and entities, targeting Australia and other countries through malicious cyber activity, that they will be held responsible for their actions. Sanctions can have a serious deterrent effect on individual actors and entities, exposing their activities and imposing restrictions on their actions, particularly when imposed in collaboration with likeminded partners.

A publicly available guidance note on cyber sanctions (https://www.dfat.gov.au/international-relations/guidance-note-cyber-sanctions) published by the Australian Sanctions Office (ASO) outlines compliance obligations for Australians and Australian businesses under Australia's autonomous thematic cyber sanction laws. It is supplemented by a FAQ document on cyber sanctions and ransomware payments (https://www.dfat.gov.au/international-relations/security/sanctions/guidance/faqs-cyber-sanctions-and-ransomware-payments). These guidance materials include information about due diligence measures that Australians and Australian businesses could undertake to comply with Australia's autonomous thematic cyber sanctions laws.

The Government encourages victims of ransomware attacks to approach it for advice and guidance on how to deal with an attack, the Australian Cyber Security Centre in the first instance and the ASO for specific sanctions advice.

The Government's priority is to assist Australians who find themselves victims of such attacks. While the Government strongly discourages the payment of ransoms, the focus of the sanctions regime is to disrupt and frustrate the perpetrators of ransomware attacks, not to punish victims of crime. That a victim has engaged with the Government concerning the ransomware attack and/or voluntarily disclosed the fact of the ransomware payment would be taken into account in any decision to pursue any enforcement or compliance action.