Committee	Parliamentary Joint Committee on Corporations and Financial Services
Inquiry	Oversight of ASIC, the Takeover Panel and the Corporations Legislation
Question No.	051
Topic	Cybersecurity
Reference	Spoken, 3 November 2023, Hansard page 6
Committee member	Senator Deborah O'Neill

Question

CHAIR: Can you give me some insights into ASIC's incident response plan for cyberattacks or data breaches and how the organisation ensures a swift and effective response to such incidents?
Mr Day: I've got to say I'm sitting here in front of you without that brief for the first time in about six months, so I'll have to take it on notice.

Answer

ASIC has an incident response plan to detect and respond to cyberattacks and data breaches, that is led by the ASIC Cyber Security function. The ASIC Cyber Security Operations Centre (CSOC) monitors the ASIC technical environments for abnormal traffic and malicious activity, including cyberattacks. When a potentially abnormal or malicious cyber incident is identified, the Cyber Incident Response Team (CIRT) is initiated to investigate. The CIRT will determine if an event is an active cyber incident, as well as the cause and impact of the cyber incident and mechanisms to mitigate adverse damage to ASIC systems and the loss or destruction of ASIC data.

The Chief Information Security Officer (CISO) is responsible for the strategic direction of cyber security across ASIC and for oversight of the cyber incident operational response lifecycle. The CISO is also responsible for executive stakeholder engagement with the data breach response, incident management and crisis management teams.

To ensure ASIC has a swift and effective response to cyber incidents, the CSOC runs quarterly cyber incident exercises with the extended CIRT members. These events ensure ASIC has a practiced and coordinated response to various types of cyber incidents, including DDoS, malware, ransomware, and supply chain attacks before any such cyber incidents may eventuate.