POLICY RESPONSE

Notification	Triage	Containment	Harms Response	Response Closure	Post-Incident
• The victim organisation becomes aware of a cyber security incident impacting their network. • Notification of an incident is received by the Mills Oakley Cyber Watch Office (MO CWO).	• The MO CWO provides legal and cyber specialists to triage the incident. Relevant parties are invited to attend as required. • Triage enables the MO CWO to deploy specialist capabilities where needed.	• MO CWO coordinate response to the immediate harms of the incident, across established lines of effort. • SITREPs are issued to relevant parties to ensure maximum situational awareness.	• MO CWO lines of effort to restore business as usual activities. • Victim organisation is supported with specialist legal, communications and technical advice relevant to the incident.	• Once business as usual is restored, MO CWO declares ‘all clear’ and monitors the situation. • A Response Closure Report (RCR) is prepared for the victim as an enduring record of events.	• MO CWO issues the RCR, with recommendations for the next 12 months. • A lessons learned process is facilitated through the RCR, with a 12-month action plan for the Victim Organisation.
OUTPUTS				OUTPUTS	
• A First Aid Call and Initial Notification within 30m of notifying MO CWO. • A Threat Assessment of the situation to inform the complexion of the response team.	• An initial Situation Report (SITREP) detailing the nature, scale and impact of the Incident, with a clear pathway forward with defined action items.	• Eradication of the Threat Actor from impacted networks. • Ongoing SITREPs detailing progress against each Line of Effort.	• Legal advice to address each specific harm or potential harm arising from the incident. • Specialist support relevant to each harm, including brand and reputation management.	• Root cause assessments to determine source of Incident. • Ongoing access to specialist capabilities in a high-care period. • Observations highlighting opportunities for uplift.	• An accessible ‘next-steps’ action plan to build resilience over a 12-month period. • A report detailing the life of the Incident, actions taken and legal advice provided to serve as an enduring record.

Digital Forensic Services

UNIT 42 BY PALO ALTO NETWORKS

McGrathNicol

Procare cyber

GRIDWARE

Crisis Communications

Arize

Forensic Accounting Services

bakertilly

Cyber Crime

KordaMentha

Barristers & Chambers

12 WENTWORTH SELBORNE CHAMBERS