Submission from Dragos, Inc. Regarding the formation of the CIRB.

For ICS/OT environments, incident response plans — spanning people, process, and technology — are required to be inherently different and distinct from IT incident response due to the difference in device types, communication protocols in the environment, adversary tactics, techniques, and procedures (TTPs), and the impacts or consequences resulting from a cybersecurity incident. The Five Critical Controls for World-Class OT Cybersecurity detail the need and reasoning for procedures specific to critical infrastructure as opposed to IT environments.

Question 20: What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?

The purpose of the Cyber Incident Review Board (CIRB) should be to comprehensively analyze cybersecurity incidents, especially those impacting operational technology (OT) environments within critical infrastructure sectors. The scope must prioritise incidents with significant or potential impact on public safety, national security, and economic stability, given that OT (i.e. industrial and critical infrastructure) cybersecurity incidents are significantly more likely to be severely impactful to large sections of the population and more likely to be of national significance. Understanding the implications and extracting meaningful lessons learned requires specific and uncommon subject matter expertise in industrial cybersecurity and critical infrastructure operation, as well as protection and resilience of both.

Question 24: Who should be a member of a CIRB? How should these members be appointed?

Membership within the CIRB should consist of individuals with proven independent expertise in industrial control systems (ICS), OT cybersecurity, incident response, and critical infrastructure protection and resilience. Representation from academia, industry, and government agencies is essential to provide diverse perspectives and diversity of thought. Members should be appointed based on merit, experience, and demonstrated commitment to advancing industrial cybersecurity resilience. A transparent and objective appointment process should consider track records, technical proficiency, and contributions to the field of OT cybersecurity.

Question 25: What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?

CIRB members should possess deep understanding and experience in OT cybersecurity, ICS, threat intelligence, and incident response methodologies. Domains of expertise required for the CIRB to be effective include ICS cybersecurity and operation, including safety considerations, threat hunting, digital forensics and incident response, risk management, and policy development. Given the unique nature of OT cybersecurity incidents, specific subject matter expertise is necessary to ensure credible incident reviews and meaningful insights for enhancing national cyber resilience in critical infrastructure sectors.

Seth Enoka, Principle OT Incident Responder, Dragos
Hayley Turner, AVP APAC, Dragos

26 February 2024