Our Data Protection Incident Response Framework

As we continue to expand Cisco's data protection and privacy landscape, we're committed to providing a transparent view into our Data Protection Incident Response Framework. Part of this framework is our Data Protection Incident Reference Guide ("IR RG").

The Data Protection Incident Response ("DP IR") team responds to data incidents leveraging pre-established and documented inter-company workflows and our Incident Response Reference Guide with documents resolution procedures and contacts. The DP IR team also drives compliance with contractual and regulatory data breach notification requirements.

The IR RG is used during the response to data incidents. It defines the process and workflow to be followed, along with lessons learned from previous data incidents.

The DP IR reference guide outlines the following:

1. The data incident workflow: A workflow that includes IR roles and responsibilities, and a structured response to data incidents to enable consistent research and action.
2. Incident reporting and triage: Defines how we manage, research, and assign the necessary action to data incident reporting based on IR case submission via our DP case tool. This will also include how we categorize each case from low to critical, along with our escalation process.
3. Managing internal and external IR communications:
   a. Internal Communications are issued by the Incident Commander and provide a periodic summary update to team members and key stakeholders.
   b. External Communications must be approved by Business-Critical Communication, the Chief Security & Trust Officer and Cisco Legal.
4. Workflow diagrams depict:
   a. Events from multiple sources and event records submitted via the DP IR case tool
   b. Initial Incident Triage Team structure, led by the DP Incident Investigator who identifies the resources to assist in impact assessment of the situation prior to the investigation
   c. Incident investigation management that determines the scope of the data exposure, who had access, and who viewed the data, the event time frame and incident severity settings
   d. Incident Management Team Triage assembly based on incident severity and enabling development of a Containment Plan
   e. Response Plan development which incorporates steps to address all aspects of the incident
   f. Response Plan execution, outlining how to define Response Plan actions, from initiation through completion, led by the Incident Commander

Our commitment to data protection and privacy does not stop with contractual terms and conditions. Cisco is also focused on:

- Developing standards and processes to define the personal data lifecycle and help ensure data transparency, accuracy, accessibility, completeness, security and consistency
- Maintaining an inventory and data map to identify what we have, what we are doing with it, where it is, where it flows and who has access to it
- Understanding data risks and conducting threat modeling for the data sets we process; improving and enhancing an enterprise-wide data incident response process that is integrated with our business continuity processes
- Integrating data protection, privacy and security requirements into product design and development methodologies
- Staying up to date on certifications such as APEC Cross Border Privacy Rules (CBPRs), Privacy Recognition for Processors (PRP), EU-US and Swiss-US Privacy Shield frameworks and maintain approvals for our Binding Corporate Rules across the EU

For more information, visit the Trust Portal.