CR2
COALITION TO REDUCE
CYBER RISK

Coalition to Reduce Cyber Risk Statement of Support for the G7 Data Free Flow with Trust Initiative

The Coalition to Reduce Cyber Risk (“CR2”) supports the G7’s initiative to promote and implement Data Free Flow with Trust (“DFFT”). In order to fulfill the promise of DFFT, however, it must be implemented in a manner that supports and gives due recognition to the criticality of global flows of security telemetry to the international cybersecurity ecosystem.

CR2 is a multi-sector, member-led nonprofit focused on promoting best-in-class approaches to cybersecurity risk management globally. CR2 members have a presence in almost every country around the world. As such, the DFFT initiative directly affects the various cybersecurity and resiliency efforts that CR2 members engage in.

Global flows of security telemetry underpin the efforts of our members to discover, identify, track, and disrupt various types of malicious cyber activity from both state and non-state cyber threat actors. Among the ways that free flow of data directly contributes to international cybersecurity and resiliency are:

- Preventing credential harvesting attacks and account compromise through the triangulation of data from different countries;
- Financial fraud prevention, through real-time data analysis and access to training data to identify global fraud trends and patterns;
- Supply chain and ransomware attack response, through global data aggregation to identify malware variants and more rapidly understand the threat they pose;
- Botnet mitigation, through improved botnet visibility that allows for the targeting and disruption of key botnet infrastructure;[1]
- Geopolitical conflict resiliency, by aiding in the “[disbursement] and [distribution] of digital operations and data assets across borders and into other countries.”[2, 3]
- Rapidly identifying and blocking new malware variants through the use of Artificial Intelligence; and
-

It is critical that these and other uses are not negatively impacted by proponents of laws and

[1] https://blog.lumen.com/emotet-redux/?utm_source=referral&utm_medium=black+lotus+labs+page
[2] https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
[3] https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

regulations that seek to limit data flows under the misconception that data localization enhances security.

CR2 supports the G7’s work, and we hope that the issues raised above will inform the continued operationalization of the “Data Free Flow with Trust” initiative so that cybersecurity and resiliency are adequately supported. CR2 welcomes the opportunity to work with G7 governments through an Institutional Arrangement for Partnership (IAP) to strengthen understanding of cybersecurity interests in global security telemetry flows and develop ways to foster trust while enabling such flows.

We support efforts to harmonize global approaches to cybersecurity, leveraging risk-based approaches and international standards, as a foundation for facilitating the flow of data and trust between stakeholders. We also recognize opportunities to foster trust by providing greater transparency into why global security telemetry is critical to enabling defense and resilience, especially given our global, dynamic threat environment.