ACCRA CALL ACTION STORIES

INSTITUTE FOR SECURITY AND TECHNOLOGY (IST)

PLEDGE: ACTION 11

Why does the Accra Call matter to your organization and your community?

The Institute for Security and Technology (IST)'s mission is to "**unite technology and policy leaders to create actionable solutions to emerging security challenges.**" The Accra Call's focus on cross-sector engagement affirms this goal and aligns with our belief that meaningful progress in cybersecurity depends on diverse perspectives and shared action.

In joining this global initiative, we are reaffirming our **commitment to building effective and inclusive approaches to cyber issues**—reflected in efforts like the Brazil Ransomware Task Force—and contributing to a more resilient and secure digital environment.

The Accra Call has shaped our approach to cyber capacity building by emphasizing the importance of inclusive, multi-stakeholder collaboration and public-private partnerships. Specifically, the Accra Call's focus on fostering stronger partnerships and better coordination, strengthened our commitment to building frameworks that are both locally grounded and globally informed.

How has the Accra Call inspired you to take action?

A key example is the development of the Brazil Ransomware Task Force (RTF), a multi-stakeholder effort led by Brazil's Ministry of Foreign Affairs and the Organization of American States (OAS), and supported by IST's expertise and efforts. Grounded in four pillars—Deter, Disrupt, Prepare, and Respond—the Brazil RTF convenes approximately 60 representatives from across government, industry, academia, and civil society to co-develop practical, context-specific strategies for ransomware resilience.

In line with the Accra Call's emphasis on equitable participation, the Brazil RTF process was designed to be **community-informed**, including a public consultation conducted in Portuguese to ensure broader access and input. The final Brazil RTF report, to be released in mid-2025, will present recommendations tailored to Brazil's national context while contributing to regional and global ransomware resilience.

Concrete achievements

- In partnership with the Brazilian Ministry of Foreign Affairs and the OAS, we convened a two-day, in-person **Brazil Ransomware Task Force conference** in Brasília. During the conference, we facilitated working group sessions and cross-pillar discussions to develop and refine national ransomware response recommendations.
- Collaborated on a **public consultation** (in Portuguese) to gather input from Brazil's broader **multi-stakeholder community**, including government, industry, academia, and civil society.
- Final Brazil Ransomware Task Force **report, with actionable recommendations**, to be published by the end of Q2 2025.