Carnegie Mellon University
Software Engineering Institute

National CSIRTs: The SEI's Role in Fostering International Cybersecurity Collaboration

MANY DEVELOPING COUNTRIES LACK EFFECTIVE COORDINATION of cyber incident response (IR) with other nations. They often respond to cyber incidents in isolation, hindering the exchange of vital information and learned practices.

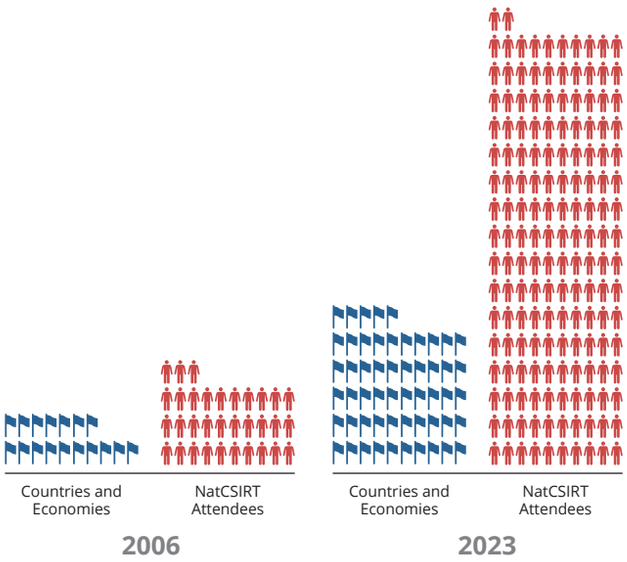
To compound the problem, these countries, which often face workforce retention issues and limited funding, mistakenly believe that strong cyber defense requires advanced IR capabilities, when simply gathering and sharing information about cyber threats is an effective approach.

These issues underscore the need for a multinational IR community that promotes collaboration and helps resource-constrained countries.

For nearly two decades, the SEI has supported a global community of computer security incident response teams (CSIRTs) for whole nations or economies and their critical infrastructure sectors. To build international IR capacity, the U.S. State Department relies on the SEI to identify national CSIRTs, help them improve their capabilities, and sponsor them for membership in the Forum of Incident Response and Security Teams (FIRST). Membership in FIRST, the premier organization and recognized global leader in IR, gives IR organizations access to a sizable network of peer organizations and best practices from all sectors. As of 2023, 9 SEI-sponsored national CSIRTs have attained FIRST membership.

Members of the national CSIRT community can teach one another to create norms by sharing how they identify, resolve, and mitigate cybersecurity incidents. This community-based approach encourages participation at all levels, including developing countries that lack resources for creating the biggest, best-funded, or most mature solutions. In the last eight years, the SEI has identified IR team members from developing countries.

Community members drive the agenda of the SEI-sponsored Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT), which occurs concurrently with the annual FIRST conference. The meetings provide a forum for national CSIRT staff to freely discuss information sharing, cyber threat intelligence, and tools.



National CSIRTs: The SEI's Role in Fostering International Cybersecurity Collaboration

Since the inception of the NatCSIRT meeting in 2006, attendance has surged from 33 to 162 and broadened its reach from 17 to 55 countries and economies. The SEI remains committed to fostering the continued growth of the NatCSIRT community and empowering the involvement that makes it a global community of trust.

The SEI, as a trusted authority in IR, provides guidance that helps countries form national and sector IR teams and scope their work given their resources. This novel approach helps resource-constrained developing countries address cybersecurity.

The SEI's work with the NatCSIRT community supports Pillar V of the U.S. National Cybersecurity Strategy, which directs public and private sectors to work with U.S. partners and allies in developing cybersecurity norms. This national strategy not only helps ensure U.S. cybersecurity but also strives to improve the cybersecurity of nations and regions around the world.

About the SEI

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu