Information Sharing to Manage Cyber Incidents: Deluged with Data Yet Starving for Timely Critical Data

Sanjay Goel
School of Business
University at Albany, SUNY
Albany, New York

Charles Barry
National Defense University
Washington, DC

Cyber security incidents that degrade user security and access to the Internet are often international in nature, simply because of the distributed borderless nature of Internet traffic flows. Effective incident response management involves detection of the breach, blocking the perpetrators from damage or theft, and identifying those responsible for prosecution. Defense against cyber threats requires the ability not only to detect breaches, but also to contain them quickly and remedy the vulnerabilities that were exploited. The robust exchange of threat and vulnerability information across organizations can improve collective national security. Development of situational awareness capability during incidents requires the collection of data from log files, both on the victim organization’s and the attackers’ servers, through Internet Service Providers that may not even be in the same country. Sharing of relevant data among responders is important both for broad participation and timeliness. No less important is close cooperation among public and private-sector actors; those essential to successful response, but also those who may become the future victims of cyber incidents, both systemic and malicious. Success means ameliorating the effects of causal factors as rapidly as possible, and restoring critical systems to full operation. Information sharing is a monumental task encumbered by administrative morass, and, often by our inability to pinpoint the precise data needed.

This paper explores the current methods of international information sharing across both private and public-sector organizations. It examines what information is critical to be shared initially, and then on a continuing basis during incident response. The paper provides a critical assessment of the hurdles still to be overcome before broad and timely sharing of information can become a reality. Finally, it offers options for improving the identification of what characterizes essential data within the overwhelming data volume of the Internet, and methods for sharing such data among responders. The salient conclusions are that: cooperation in cyber incident response, while well recognized, is in its infancy in terms of identification of critical data to be shared; effective information sharing is the rare exception rather than a well-established practice; and the primary hurdles remaining are human factors not technological inadequacy. The long-term strategy for information sharing requires streamlining the administrative process, standardizing formats for data exchange, and creating specific data collection requirements for organizations as well as Internet operators. The paper concludes with recommendations for future of information sharing among organizations.

The full version will be made available online through the ASIA website at: http://www.albany.edu/iasymposium