Cyber Resilience Economics Workshop, call for papers

This proposed workshop will be co-located with QRS 2016 (http://paris.utdallas.edu/qrs16/), the 2016 IEEE international conference on Software Quality, Reliability, and Security, in Vienna, Austria August 1-3, 2016.

Background and Scope: Cyber economics drives many of the decisions related to cybersecurity by both the defenders and attackers. It determines on the defensive side the technologies and procedures implemented to prevent and respond to cyber-attacks. On the offensive side, it not only determines the type of attack but also the effort expended to ensure its success. In short, it determines the asymmetric balance between the attackers and defenders. The Cyber Resilience Economics workshop will explore effects of cyber economics on this asymmetric balance and examine approaches to shifting adversaries' current advantage in cyber conflicts in favor of defenders. It will bring together a diverse group of experts to advance the concepts and application of cyber economics as related to asymmetric advantage and cyber resiliency. This includes foundational and applied advances in economics, its effects on asymmetry and resiliency driving the essential system requirements for cyber systems including traditional IT, cloud platforms, cyber-physical systems, and critical infrastructure. This will serve to accelerate the recognition, adoption and application of cybersecurity resilience within industry, government and academia by addressing the key concerns of how these techniques and technologies can be realized within the practical constraints of cost, risk, and benefit.

Information for Authors: We are currently seeking manuscripts for a ½ day workshop that will be a forum to discuss recent research in areas associated with cyber resilience economics. Manuscripts should be submitted in the IEEE standard conference format of 8 pages maximum in the following topics of interest:

- Foundations of asymmetric cyber advantage
- Defining practical cyber resiliency
- Technical & architectural approaches to gaining asymmetric advantage
- Metrics, measures, and economics of cyber resiliency & asymmetry
- Optimal balance between resiliency and security
- Adversary economics: assessing the value of impacting the attacker
- Frameworks for ROI analysis (cost, risk, benefit) to guide technology investment (research, development, and utilization)
- Integrated analyses of cyber resiliency & asymmetry with co-dependent infrastructures (e.g., power)
- Cyber resiliency related tools that are guided by economic factors for defender and/or adversary
- Use cases or case studies for defender and/or adversary that include economic factors

Chairs:
Nick Multari (PNNL) nick.multari@pnnl.gov
Jeffrey Picciotto (MITRE) jp@mitre.org

Steering Committee:
Tyler Moore (Univ. Tulsa) tyler-moore@utulsa.edu
Christopher Oehmen (PNNL) chris.oehmen@pnnl.gov
Rosalie McQuaid (MITRE) rmcquaid@mitre.org
David Manz (PNNL) david.manz@pnnl.gov
Richard Graubart (MITRE) rdg@mitre.org
Pradeep Ramuhalli (PNNL) pradeep.ramuhalli@pnnl.gov
Deborah J. Bodeau (MITRE) dbodeau@mitre.org

Key Dates:
Manuscripts Due: April 29, 2016 (Extended)
Author Notification: May 25, 2016
Camera-ready and author registration due: June 10, 2016
Conference dates: August 1-3, 2016