2nd Annual International Workshop for Cyber Resilience Economics Call for Papers

This proposed workshop will be co-located with the 2017 IEEE International Conference on Software Quality, Reliability, and Security (http://paris.utdallas.edu/qrs17/), in Prague, Czech Republic, July 25-29, 2017.

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, these and other factors determine the asymmetric balance between the attackers and defenders. The Cyber Resilience Economics workshop will explore foundational and applied advances to achieve an optimal asymmetric balance and how to most effectively leverage technical and management options to achieve this target. To do so, the workshop will seek to understand the parameters needed to accurately quantify asymmetric imbalance from both the offensive and defensive perspective; examine technical and non-technical approaches to shifting that balance, including the full range of costs/benefits of each approach; and explore and evaluate a range of options for defining and achieving optimality. It will bring together a diverse group of experts to advance the concepts, analysis and application of cost, value, risk and other important features of cyber systems as related to asymmetric advantage and cyber resiliency. This will serve to accelerate the recognition, adoption and application of cyber 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.

We are currently seeking manuscripts for a full-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 specific topics of interest to include, but not limited to:

- Foundations of asymmetric cyber advantage
- Integrated analyses of cyber resiliency & asymmetry with cyber environments
- Metrics, measures, and economics of cyber resiliency & asymmetry
- Defining practical cyber resiliency
- Technical & architectural approaches to gaining asymmetric advantage
- Relationship between resiliency and security
- Adversary economics: assessing the impact of defender capabilities and actions to the attacker
- Frameworks for ROI analysis (cost, risk, benefit) to guide technology investment (research, development, and utilization)
- 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

In light of the interactions and interdependencies of today's cyber infrastructures, the scope of this workshop is to explore the above topics across the full spectrum of cyber systems to include traditional IT, cloud platforms, cyber-physical systems, Internet of Things, operational technologies, and critical infrastructure.

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

Key Dates:

Manuscripts Due: April 21, 2017 (extended) (http://banana.utdallas.edu/qrs2017/start/www/CRE2017/)
Author Notification: May 25, 2017
Camera-ready dues: June 5, 2017
Workshop: July 25-29, 2017