CHALLENGE

Cyber defenders have many different perspectives and motivations, both across and within organizations. Some are motivated by business volume and sales while others are motivated by risk. Simultaneously, IT professionals are more interested in making sure systems work properly than in kicking people off the network. From planning to execution, each of these perspectives is critical for effective cyber defense. However, these functions typically operate in silos and are lacking crucial communication pathways. Pacific Northwest National Laboratory’s (PNNL) tabletop training and coordination tool, known as Dorci, addresses this issue both within and across organizations, helping to optimize cyber defense in resource constrained environments.

APPROACH

Dorci allows players to assume specific roles and move together through a cyber scenario. A subject matter expert facilitates the game while individuals in the different roles are required to coordinate their cyber defense, balancing various responsibilities including business, defense, engineering, and intelligence. Realistic responses delivered by the facilitator have impacts on how the game plays out, enabling cyber defenders and IT professionals alike to understand the complexity and effect of each decision. Players can assume their current role or take on a new perspective to enhance their understanding of the different functions.
of cyber defense within their organization. The game is also available for multiple teams to play simultaneously, enabling coordination across organizations.

**METHODOLOGY**

This tabletop exercise is a semi-scripted red team activity facilitated by a subject matter expert game master. However, the script is dynamic and interactive; the activities of the red team are dependent upon the decisions made by the defending team.

A team of defenders makes coordinated decisions using cards and tokens to represent funds and resource constraints. These parameters allow users to assess the cost of specific decisions or technology implementations, and the complexity of the decisions while evaluating the effectiveness of such choices through an attack scenario. Playing multiple games simultaneously allows users to play through scenarios of information sharing across institutions in an effective manner.

**IMPACT**

PNNL’s tabletop training and coordination exercises facilitate communication between cyber defenders of different roles and perspectives. Establishing these critical communication pathways enables information sharing within and across organizations, leading to more effective cyber defense from planning to execution. Specific applications include:

» **High-value asset protection.** A more coordinated response to cyber conflict amongst critical infrastructure and military asset owners and operators.

» **Cross-training.** Training non-cyber specialists to be more aware of how cyber conflict happens, enabling them to make informed decisions that may affect cyber response.

---

**Contact**

**Rick Riensche**  
Principal Investigator  
509-375-4535  
rmr@pnnl.gov

**Chris Oehmen**  
Initiative Lead  
(509) 375-2038  
chris.oehmen@pnnl.gov

**Pacific Northwest National Laboratory**  
Proudly Operated by Battelle Since 1965