



Lab hosts multi-lab cyber security games

April 12, 2012



LOS ALAMOS, New Mexico, April 12, 2012-Intense pressure creates diamonds from coal, they say, and for Department of Energy (DOE) national laboratory cyber security programs, it's an apt comparison. Fending off thousands of computer attacks from around the world, controlling vast libraries of sensitive information, yet keeping the scientific flow of knowledge moving, cyber teams such as those at Los Alamos National Laboratory (LANL) and elsewhere in the government complex feel the squeeze.

Sharing insights and ideas from the teams' experiences, however, can create a boon in cyber defense and incident management, and potentially provide useful input for other government agencies such as the new federal Joint Cyber Coordination Center, or JC3. The JC3 is focused on improving the national response to threats, leveraging complex resources, and sharing information to meet information security commitments to the nation.

Recently, Los Alamos National Laboratory hosted an information security exercise dubbed “Eventide” that put more than 100 participants from around the complex into a virtual maelstrom of bad news and worse events, as the simulation spewed sensitive data and cracked network security out into the wilderness of the internet. They had to assess what was happening and how to respond, as their systems were progressively compromised, sensitive data appeared on hostile web sites, and invisible “bad guys” revealed their nefarious plans.

“That was pretty scary... but most E-ticket rides are,” said one participant.

Coordinated by Dale Leschnitzer, LANL's “master of disaster,” Eventide brought together cyber and IT leaders from 20 sites, including the Federal Bureau of Investigation, the DOE, its Cyber Forensics Laboratory and National Nuclear Security Administration, and the DOE’s national laboratories, to develop recommendations on resources they need from JC3. Not only did Eventide set the stage for the complex to ask the hard (and realistic) questions, it also acted as an excellent incubator to assist the JC3 in developing a practical path forward.

Tom Harper, LANL’s chief information officer, said: “Cyber threats target our information and data, and our productivity through vulnerabilities in our IT infrastructure. They pose great risks to our organization’s security and the nation's competitiveness.”

Harper said: “We’ve had a trial by fire and it’s toughened our teams. Now we can strengthen and optimize our joint defenses to ensure we’re a national resource ready to develop responses and templates to assist government and industry.”

A player describing himself only as “a DOE detailee” pointed out that “we’re all under attack, and now we can help each other. We’ve got a lot of smart people here, and when it comes to cyber, the government’s light years ahead of much of the industry, for good reasons. Asking the tough questions makes you think. This is why you train on real attacks and valid scenarios. It’s our chance fill the voids.”

Harper noted that the past years’ work has been to improve the Laboratory’s posture and, to a degree, misperceptions about LANL’s capabilities on these issues. Harper is chairing the National Laboratory CIO Council for 2012, in which chief information officers from across the complex are working with the federal employees to ensure that defense and response are agile and proactive, and that the focus is on agility, leveraged resources, and information sharing.

“Eventide was the way to maximize input to plans by cyber and IT leaders from DOE’s national laboratories and plants,” Harper said.

Los Alamos National Laboratory

www.lanl.gov

(505) 667-7000

Los Alamos, NM

Operated by Los Alamos National Security, LLC for the Department of Energy's NNSA

