# California May Incorporate Cyber-Readiness into State Emergency Plan

Hilton Collins | May 11, 2011

SACRAMENTO, Calif. — California could take cyber-security preparedness to a new level — state officials are considering adding cyber-readiness to the state emergency plan alongside other disasters that could endanger citizens and infrastructure. Keith Parker, acting chief information security officer for California's Office of Information Security, did not mention any barriers to completion, but said the process, which involves his office working with the state's Emergency Management Agency, could take a while.

"We'll be the first in the nation if we can mature this to fruition," Parker said.

Parker announced this and other state business during a seminar on Tuesday, May 10, at the Government Technology Conference West, an annual event hosted by e.Republic Inc., *Government Technology* magazine's parent company.

Parker also spoke of state plans to consolidate servers, including e-mail servers. Consolidation efforts will help IT leaders manage and secure state data more easily, something that's essential for a network that faced constant attacks last year. State government comprises more than 150 agencies, more than 1,000 ca.gov domains and more than 175,000 e-mail boxes.

California experienced legions of potential breaches in 2010 alone, which were all detected by IT. Man-in-the-middle, cross-site scripting and Trojan attacks were among them.

Attack types included:

- 8.5 million blocked malware activities;
- more than 1,700 reported security incidents, which were all successfully detected by IT;
- 55 suspicious activity notifications;
- 26 keylogger notifications; and
- 246,393 breach notifications.

According to Parker, one agency's weakness could be every agency's weakness because of how interconnected they all are in today's networked environment. "We have hundreds of thousands of state employees, so we have hundreds of thousands of attack vectors," he said.

He began his presentation with a video showing the federal government's response to Cyber ShockWave, a simulated cyber-attack test exercise lawmakers participated in last year. In the simulation, a smartphone-based botnet attack that was launched by foreign criminals hit the United States and participants didn't seem prepared to mitigate the threat. "There was never a solution to this exercise," Parker said.

But he added that it's spurred action and discussion: legislation is currently being crafted, though nothing has become a law yet. These include the controversial Internet kill switch bill that senators introduced in 2010. Parker spoke of the Pentagon recognizing cyber-space as the fifth domain of the military, along with land, sea, air and space.

According to Parker, his office is California's representing agency to the Multi-State Information Sharing and Analysis Center and works with the federal government in the interest of national cyber-security. He hoped his Government Technology Conference audience would walk away from his speech cognizant of the fact that multiagency collaboration is important to cyber-security and that citizens must understand how important securing network infrastructure is.

http://www.govtech.com/policy-management/California-May-Incorporate-Cyber-Readiness-into-State-Emergency-Plan.html