



Home Authentication / Biometrics Business / Finance Continuity / Recovery Cybersecurity Detection Education / Sci-Tech Emergency / Police / Mil. Government policy
Infrastructure Public health / Biodefense Surveillance Systems integration Transport / Border

THE BUSINESS OF HOMELAND SECURITY

Thursday, 13 May 2010

ADVERTISE [SIGN UP FOR OUR FREE DAILY REPORT](#)

 Search

Cybersecurity summit pays little attention to control system's security

Published 13 May 2010

Despite threats of infrastructure attacks, scant attention was paid to control systems during a global security conference; the problem is safeguarding infrastructure's control systems against attackers is that such protection requires a different approach to securing PCs or networks; Windows-based security products will not help; says one expert: "All the devices that sense things -- temperature, pressure, flow, and things like that -- are not Windows, those are proprietary, real-time or embedded, and there's no security there"

As online attacks increase in severity and reach, targeting everyone from Google to the Pentagon, leading security experts and government officials met last week in Dallas at the EastWest Institute's first annual [Cybersecurity Summit](#).

The goal of the conference was to find common solutions to cybercrime and other online attacks, which respect no national boundaries. *InformationWeek's* Mathew Schwartz [writes](#) that the first step, then, was to introduce policymakers and experts from around the world, to begin creating the relationships and transparency needed to make this happen. "How can you do partnerships with private industry, how can you do it with other governments when everything's behind a veil of secrecy?" said White House Cybersecurity coordinator Howard Schmidt.

The next step, Schwartz notes, will be more challenging. "Breakthrough solutions will require the effective integration of technical, business, legal, defense and international policy competencies on a level that has not happened so far," wrote attendee Ikram Sehgal, a defense and political analyst and EastWest board member, in the *News*, a Pakistani newspaper. "Nations are thinking too parochially about their online security to collaborate on crafting global cyber regulations."

Top of the cybersecurity agenda for many governments: how to prevent "nightmare" infrastructure attacks against "electricity, power grids, transportation, airplanes, water supply, finance, the banking system [and] the health system," said Patrick Pailloux, director general of the French Network and Information Security Agency. His biggest nightmare? "That we don't have enough time to prepare us for the nightmares."

Such infrastructure attacks are ongoing, and at least in the United States, on the increase, said retired Air Force lieutenant-general Harry Raduege, now chairman of Deloitte's Center for Cyber Innovation. "We have experienced a number of attacks against the financial sector, on the power grid and against our defense capability." Schwartz writes that curiously, given the infrastructure worries, of the roughly 450 invited attendees present, only one hailed from the industrial control systems community, said critical infrastructure security expert Joe Weiss. "I was the one. That's absolutely typical — there wasn't one single electric utility there, not even the one headquartered in Dallas, and there wasn't one single control system supplier."

At issue — for a meeting intended to find global solutions to information security challenges — is the fact that safeguarding control systems against attackers requires a different approach to securing PCs or networks. For starters, Windows-based security products will not help. "All the devices that sense things — temperature, pressure, flow, and things like that — are not Windows, those are proprietary, real-time or embedded, and there's no security there." Furthermore, seemingly rote IT activities, like installing antivirus on a control system, can actually create a denial of service. "Who needs hackers?" he said.

Infrastructure defenders, stay tuned: After bringing the above disconnect to the summit organizations' attention, Weiss received an assignment: to get the control systems community involved in next year's Cybersecurity Summit in London.

Topics: [Corporate IT security](#) | [Firewalls](#) | [Network security](#) | [Infrastructure protection](#)

IN TODAY'S REPORT

- [Insurers refuse to cover journalists working in Ciudad Juárez, Mexico](#)
- [Cruise ships may be required to hand over passenger reservation data](#)
- [New method to develop latent fingerprints](#)
- [BP tries new, smaller capping device to plug Gulf gusher](#)
- [Sensors emulate insects' acoustic capabilities](#)
- [General Dynamics acquires explosives disposal specialist](#)
- [Will the World Cup change South Africa?](#)



H Home Authentication / Biometrics Business / Finance Continuity / Recovery Cybersecurity Detection Education / Sci-Tech Emergency / Police / Mil. Government policy Infrastructure Public health / Biodefense Surveillance Systems integration Transport / Border
About us Sign up Advertise Contact Privacy policy

2009-2010 © News Wire Publications, LLC