

CNET News

[Politics and Law](#)

March 19, 2009 11:58 AM PDT

Senator plans to promote cybersecurity education

by [Stephanie Condon](#)

- Font size
- Print
- E-mail

WASHINGTON--The U.S. economy is suffering massive losses every year due to cyberattacks, yet most Americans are not aware of the problem, cyber experts told Congress Thursday. Without more federal funding for educational reforms and basic research to promote cybersecurity, the nation will regularly suffer from attacks of serious consequence, they said.

"We've had our electronic Pearl Harbor," said James Lewis, a senior fellow at the Center for Strategic and International Studies. "We're trying to figure out how many people have figured out this is a major national security problem, and I don't think enough have."

Seemingly in demonstration of Lewis' point, he and the three other cybersecurity experts testifying before the Senate Commerce, Science, and Transportation Committee on Thursday had a small audience--no more than three of the committee's 25 senators were in attendance at a time.

"I'm mortified by the lack of attendance," said Committee Chair Jay Rockefeller (D-W.Va.) "I regard this as a profoundly and deeply troubling problem to which we are not paying much attention."



He insisted he will aggressively press the subject with more hearings, as well as a bill he will introduce with Sen. Olympia Snowe (R-Maine) that will, among other things, provide funding for scholarships to get more people into the field of cybersecurity.

While Congress has dedicated a number of [hearings](#) over the past year to cybersecurity, Thursday's meeting focused specifically on the damage the private sector incurs from cyberattacks.

"The commercial losses are in the tens of billions of dollars a year," said Eugene Spafford, a professor and the executive director of Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS). "Imagine a Hurricane Katrina-style event occurring every year and being ignored."

Furthermore, he said, the criminals who profit from cyberattacks are reinvesting their money in new tools to conduct more attacks--far more than the United States invests in defensive tools.

The federal government, Spafford said, should invest more in basic research to fundamentally redesign security systems, both for the purpose of creating better systems but also to strengthen the country's level of cybersecurity expertise.

"Our investments in research, even if they don't always produce something we can use, do have a benefit in the country's knowledge base," he said.

Expertise is especially lacking in the area of industrial control systems, said Joseph Weiss, managing partner for the consulting firm Applied Control Solutions. A control system, he said, is a "system of systems" typically designed by an engineer rather than a computer scientist.

"I believe less than 100 people worldwide truly know and understand control system cybersecurity," he said.

Control systems, he said, are designed as simply as possible so they perform more reliably, but are consequently more vulnerable to cyberattacks. An attack on such a system would take the country "months--not days"--to recover from, he said.

Rockefeller expressed disbelief that more students were not interested in pursuing careers in cybersecurity.

"This ought to be the most fascinating, cerebral problem that exists," he said. "It just cries out for the smartest, most creative people."

Sen. Maria Cantwell (D-Wash.), one of the few other senators in attendance, said some of the people who have built careers in finance would have done more good in cybersecurity.

"It is pretty disgusting we've had more people cooking up toxic assets than killing bugs" on networks, she said.

The witnesses at the hearing said the economic downturn driven by those toxic assets has only increased the risk of cyberattacks. They cited the case of a disgruntled information technology worker [indicted](#) Tuesday for allegedly sabotaging a computer system he helped set up for a California oil and gas company, after he was not offered a permanent job.



Stephanie Condon is a staff writer for CNET News focused on the intersection of technology and politics. She is based in Washington, D.C.
[E-mail Stephanie.](#)

Related

From CNET

[Obama's budget blueprint enhances cybersecurity](#)


[Defense contractors eye cybersecurity bonanza](#)

[Year in review: Scams up, but big Net attack averted](#)

From around the web

[Cybersecurity director resigns amid turf...](#) AOL News - Politics

[Cyber director resigns amid federal turf...](#) AOL News

[More related posts](#) powered by  Sphere