c|net NEWS.COM http://www.news.com/

# Homeland Security IT chief blamed for cyberwoes

By Anne Broache
http://news.com.com/Homeland+Security+IT+chief+blamed+for+cyberwoes/2100-7348_3-6192255.html

Story last modified Thu Jun 21 10:34:00 PDT 2007

**WASHINGTON--In response to reports of persistent cybersecurity flaws at the Department of Homeland Security, a top congressional Democrat on Wednesday questioned whether the agency's chief information officer deserves to keep his job.**

The department charged with safeguarding the security of the nation's computer systems has not been setting a good example and CIO Scott Charbo hasn't shown he's serious about fixing its vulnerabilities, said Rep. Bennie Thompson (D-Miss.), chairman of the House of Representatives Homeland Security Committee.

"How can we ask the private sector to better train employees and implement more consistent access controls when DHS allows employees to send classified e-mails over unclassified networks and contractors to attach unapproved laptops to the network?" Thompson asked at an afternoon hearing here held by a subcommittee that deals with cybersecurity issues.

He was referring to the Homeland Security department's revelation, as part of an ongoing subcommittee probe into its information security practices, that it experienced 844 security-related "incidents" on its computer systems in 2005 and 2006. Those episodes included unauthorized users hooking up personal computers to government networks, unauthorized software installations, classified e-mails traveling over unclassified networks, suspicious botnet activity, trojans and virus infections, classified data spillages and misconfigured firewalls.

Charbo, for his part, downplayed the lengthy list, saying that they didn't indicate actual penetrations of the system and varied widely in the level of severity. "Those are events that we report on as a data-gathering tool," the IT chief told the politicians, adding that he was confident all breaches considered significant had been addressed properly.

**"How can we ask the private sector to better train employees and implement more consistent access controls when DHS allows employees to send classified e-mails over unclassified networks and contractors to attach unapproved laptops to the network?"**
--Rep. Bennie Thompson (D-Miss.)

The congressional panel that convened Wednesday's hearing has been probing the extent to which various federal agencies are equipped to handle cyberthreats. At a hearing in April, committee members accused officials at the Commerce and State Departments of being ill-prepared to handle such threats in light of reports of intrusions from Chinese hackers, and they warned that Homeland Security would be undergoing scrutiny next.

Criticism of that department's cybersecurity efforts from Congress and federal auditors is hardly new. Some would argue the department has shown minor signs of improvement this year since it pulled up its federal information security "grade" from an "F" to a "D."

Even so, Government Accountability Office auditors at Wednesday's hearing said various components of Homeland Security still aren't doing enough to limit access to their systems, authenticate and identify users, encrypt sensitive data and keep logs of user activity.

The GAO is preparing to release a report based on a yearlong investigation that it says documents "pervasive" security flaws in Homeland Security's US-VISIT program, which is designed to verify the identity of foreigners through fingerprint scans and is currently being used at several U.S. ports of entry.

Keith Rhodes, one of the report's authors, said the GAO found that US-VISIT is riddled with problems "across the board," which, left uncorrected, could put sensitive personal information at risk. The flaws are mostly due to "bad configurations" that could be fixed both easily and cheaply, he said. But because of the deficiencies, there's no way of knowing whether the database associated with the computer systems has already been hacked, he said.

"I did not see controls in place that would prevent (hacking), I did not see defensive perimeters, and I did not see detections systems in place that would let you know whether it had or had not" been hacked, Rhodes told the committee.

Charbo said he and department officials were still reviewing the draft version of that report but were prepared to address the weaknesses by year's end.

Now on News.com
Web 2.0 security: 'Invent the wheel' Linux coders tackle power efficiency Special feature: The countdown to the iPhone Extra:

Artificial intelligence: Lost in the woods

On a broader level, Charbo said he realizes the agency has improvements to make but urged the politicians not to overlook what he called "significant progress" during the past few years. For instance, it has "remediated" 7,000 weaknesses identified by auditors and has certified that 95 percent of its systems have appropriate controls in place--compared with only 26 percent in October 2005.

Others questioned whether the department has been dedicating enough of its overall tech budget to security. According to Homeland Security, it spent $12.5 million in 2004, $17.5 million in 2005, and $15 million in 2006 and 2007. Charbo justified those expenditures by saying they reflected "our strategic security plan."

The lone Republican present at the hearing, subcommittee co-chairman Michael McCaul (R-Texas), said he and others were considering introducing legislation that would force Homeland Security to come up with a "national strategic threat assessment" regarding U.S. cybersecurity.

"This has never been done, it's long overdue, and the nation needs this to protect it," he said, adding that he feared a devastating cyberattack could be worse than the "effects of a weapon of mass destruction."