

## DHS official: Agencies must make high-risk cyber threats top priority

By [Jill R. Aitoro](#) 08/25/09

ATLANTA -- Federal agencies should prioritize their information security requirements to ensure mission-critical operations are protected first, and delineate between "that which is aggravating and that which is truly dangerous," the Homeland Security Department's cyber chief Greg Schaffer said during a conference on Tuesday.

Cyberattacks are growing far more sophisticated, in part because they're more difficult to detect, said Schaffer, who was appointed assistant secretary of DHS' Office of Cybersecurity and Communications in June. Schaffer and Dave DeWalt, chief executive officer of security vendor McAfee, spoke Tuesday morning at the GFirst conference in Atlanta hosted by the department's U.S. Computer Emergency Readiness Team.

"The more sophisticated attacks ...are low and slow, designed to not draw attention, but insidiously get at data and resources," Schaffer said "Yet at the same time, the level of noise from less sophisticated attacks continues to grow. This makes for an environment where it is easy to focus on the wrong pieces of the puzzle while bad things happen under the radar. We need to be vigilant and focused."

According to security vendor McAfee, there was a 500 percent increase in 2008 in the number of malware attacks that used hostile code to infiltrate or damage a computer system -- equal to the combined total for the five years prior, DeWalt said. In 80 percent of all malware attacks, the motive is financial, with attackers trying to steal identities and data for profit. The other 20 percent of attacks are prompted by "religious reasons," such as political espionage or terrorism.

McAfee also reported that 1.5 million malicious sites, which infect computers of visitors with malicious code, are created each month, and spam, which is increasingly tied to the spread of malware, increases 10 percent annually.

The challenge for agencies is determining where to focus their limited resources in such a hostile environment, said Shaffer in an interview with *Nextgov.com* after his speech.

"We have to put an appropriate level of resources to those issues" that are less critical, he said, such as a denial-of-service attack that temporarily blocks access to an agency's network or Web defacement that alters online content. "At the same time, we need to recognize that those are not the really dangerous attacks. It's a resource [allocation] issue; when you have so much attention focused on these areas that are not as critical, the less noisy attacks can" go unnoticed.

Only agencies can prioritize information security efforts based upon their individual missions, Shaffer said. Agencies also must strike a balance between security and efficiency, or minimizing network vulnerabilities, without sacrificing productivity.

"[DHS] can help set some requirements and assist in moving the ball forward, but the agencies themselves have to understand their risk profiles and execute against their mission," Shaffer said. "How do you continue to maintain

the efficiency gains that the technology presents, while at the same time incorporating an appropriate level of security so we don't get damaged?"

Agencies should apply what Shaffer called tiered-levels of security, where the degree of security applied is determined by the level of risk associated with the information maintained on the computer system. That analysis will vary from agency to agency.

"Agencies need to start understanding the networks in which they live, so they can look at their environment and say, 'I know this isn't going to have a heavy impact, so I won't focus my efforts there,' " said Randy Vickers, whom DHS named as acting director of US-CERT on Tuesday. His predecessor, Mischel Kwon, resigned earlier this month.

"We tend to focus all over the map, rather than on the key areas that could keep us from accomplishing our missions," Vickers said.

---

[COMMENT ON THIS ARTICLE IN THE FORUM](#)

---

---

© 2009 BY NATIONAL JOURNAL GROUP, INC. ALL RIGHTS RESERVED