Can Infosec Survive Big Spending Cuts?

Facing Consequences If Superpanel Can't Come Up with Plan

November 8, 2011 - Eric Chabrow

The potential is real: Congress will slash significant amounts of dollars -tens of millions or much more -from initiatives to safeguard the federal government's critical and most sensitive information and systems. In reality, however, such a dire outcome is not certain. In the end, any spending cuts on cybersecurity, if they occur, likely will have negligible impact on government IT security. But with the current government, nothing is certain.

Congress established the so-called Supercommittee to recommend by Nov. 23 at least $1.5 trillion in deficit cutting measures over a 10-year-period. If the Supercommittee - equally composed of Democratic and Republican lawmakers from both houses - fails to reach an agreement, a so-called trigger mechanism would enact $1.2 trillion in automatic spending cuts, split between the national security and domestic budgets. IT security - in all its forms - falls within both areas.

Karen Evans, the onetime top federal government IT executive - in effect, the federal chief information officer, says it's difficult to specifically name IT security programs that would be cut. "I believe you will see top-line programs cut; therefore, the supporting resources such as IT and therefore the security programs associated with them will be reduced and/or cut," she says.

If faced with these cutbacks, it's more important than ever for federal agencies to effectively implement their information risk management programs. "The reductions need to be commensurate with the risk profile for the services which the government is going to continue provide," Evans says. "Therefore, the government will continue to use IT to provide services and the agencies would plan for the appropriate cybersecurity protections with these services."

Alan Paller, research director at the SANS Institute, an IT security training organization, sees agencies **collaborating** with one another on cybersecurity to stretch limited funding. "That's good," he says.

One indication that the federal government is moving in that direction - even without the threat of funding cuts - was last week's pronouncement by Federal CIO Steven VanRoekel that all federal agencies seeking to contract cloud computing services must employ FedRAMP - the Federal Risk and Authorization Management Program - a cross-agency initiative that vets cloud providers (see ***FedRAMP to Become Mandatory***).

Military Cuts Likely

But the biggest threat to the automatic spending cuts would be in protecting the military.

Richard Stiennon, author of Surviving Cyber War and the forthcoming Cyber Defense: Countering Targeted Attacks, points out that the **Defense Department** would be forced to come up with $200 billion in cuts over each of the next four years if the Supercommittee fails to identify cuts in federal spending. But, he says, most of those cuts would likely come from major procurements of weapons systems and not from IT security.

"That said, there will be lots of cries of pain, and cybersecurity, along with other high visibility systems, will be put on the table," he says. "But the military cannot afford to neglect IT security. They have already suffered a billion dollars in recovery costs associated with Buckshot Yankee, the clean up from a USB-born malware episode. Electronic warfare systems are paying the greatest dividends right now. Perhaps cutting new weapons delivery platforms such as advanced fighters, bombers, ships and subs will be a good thing since those multi-decade programs suffer the greatest cost overruns and deliver outdated platforms too late to have a positive impact on global security. "

Operation Buckshot Yankee refers to the defense against a 2008 cyberattack characterized as the worst breach of military computers, which resulted in the creation of the U.S. Cyber Command (see ***Military Stands Up CYBERCOM as Its Latest Command***). It took the military 14 months to clean up that attack, which started when a USB flash drive containing malicious code left by a foreign intelligence agent in a DoD parking lot was plugged into a computer attached to the military's central command's IT system.

James Lewis, director of the technology and public policy program at the think tank Center for Strategic and International Studies, cites comments made Monday

at a CSIS forum by James Miller, DoD's principal deputy undersecretary for policy, that the Pentagon would do all it can to shield cyber from spending cuts. "The real problem is whether the Hill will mess up," Lewis says, referring to Congress. "After the NCIX report, they won't be able to blame 'intelligence failure.'"

NCIX refers to the federal government's Office of National Counterintelligence Executive, which last week issued a report that says the Chinese and Russians are spying on U.S. corporations over the Internet, stealing trade secrets that could prove harmful to America's prosperity and security (see ***4 Targets of Foreign E-Spying***).

And, the head of the Defense Advanced Research Projects Agency, speaking at an agency cybersecurity colloquium on Monday, says DARPA is set to increase its budget for cybersecurity research by 50 percent. "We are shifting our investments to activities that promise more convergence with the threat and that recognize the needs of the Department of Defense," DARPA Director Regina Dugan says. "Malicious cyber attacks are not merely an existential threat to our bits and bytes; they are a real threat to our physical systems, including our military systems.

Much Ado About Nothing?

Ben Friedman, a research fellow in defense and homeland security studies at the Cato Institute, a libertarian think tank, doubts that the mandatory budget cuts known as sequestration will occur. The first cuts aren't scheduled to take place until January 2013. "Neither the White House nor a Congressional majority want to sequester funds from the Pentagon, so they are likely in the interim to cut a new deal undoing the BCA or simply raising its budget caps," Friedman says. "So the effect of the Supercommittee's failure on cybersecurity programs will probably be basically nil."

Should cuts occur, Friedman says, they would be across the board, $50 billion a year, which means defense spending levels would retreat to 2007 levels. "However," he says, "cybersecurity funds has been growing faster than the whole, so they would be set back to about the amounts they were at two or three years ago. That would be less cybersecurity but no disaster given that funding is not much of a measure of security."

Friedman and other Cato scholars contend the cybersecurity threat has been hyped massively. "There is less to worry about than most would say," he says. Plus, he points out, most of the nation's critical cyber infrastructure is protected by its private-sector owners. "So," he says, "reductions in government efforts would have minor effect there at most."

Friedman's views aren't shared by many cybersecurity experts, but in the final analysis, potential budget cuts to IT security wouldn't be as severe as they would be to other programs, and the defense of government systems - civilian and military - should continue to grow.