

SIFMA OPS 2010: Market Swing “Highlights Vulnerability” to Attack by Extremists, Former NSA Director Says

May 7, 2010

Tom Steinert-Threlkeld

PALM DESERT, Calif. – The former head of the nation’s most talented set of code-breakers said Friday that the near-1,000 point plunge in the Dow Jones Industrial Average “highlights the vulnerability” of the nation’s capital markets to direct attack by extremists interested only in causing destruction.

Michael McConnell, former director of the National Security Agency, told executives attending the 2010 Securities Industry and Financial Markets Association Operations Conference that in “my personal view there is no indication” that the plunge Thursday was triggered in any fashion by an extremist attack. But ...

But, the executive vice president in the nation’s capital for consulting firm Booz Allen Hamilton, said “What it highlights is the vulnerability. So if this turns out to be a typo -- I don’t know that it will, but if it does -- you start to fathom the potential impact.”

McConnell served as director of the National Security Agency from 1992 to 1996 and the United States Director of National Intelligence from February 2007 to January 2009 during the Bush Administration and first week of the Obama administration.

At the NSA, which is charged with “breaking into other people's stuff to figure out what their secrets are,” McConnell said he learned what “we’re capable of,” and believes the capabilities to be replicable.

A “red team” of computer experts at the NSA had a “100 percent success” ratio of breaking, entering and taking control of the United States’ own information systems, at the root level, in any agency, small or large.

And, last year, he replicated that success, when he went into private enterprise.

“When I came into industry, (I said) I’m going to see if I can round up a dozen guys, with some pizzas and coke and do some penetration testing,” the Booz Allen executive said. “Our success rate was one short of being 100 percent. The one we didn’t break into was a small government agency that had one large mainframe. And the reason we didn’t take root privileges was that they unplugged it.”

He says extremist groups do not care about getting into financial systems, making copies of records and just getting out without leaving their fingerprints. Instead, they just want to cause as much damage as possible.

They can do it by linking together different like-minded individuals in Pakistan, Turkey and Germany and launching an attack from Asia, for instance.

This won’t be poorly planned or executed, like the failed bombing attempt in Times Square last Saturday. These won’t be “average guys.” Instead, the members of this attack team will be graduates of “India’s MIT” or similar caliber institutions around the globe. Or with similar smarts, perhaps using as many tools as they can that are already spread on the Web.

And it may take more than a dozen.

“Say it’s two dozen, say it’s three dozen. I don’t know what it is,” he said. “But yesterday we lost a trillion dollars in about two and a half hours.” An extremist attack likely would lead to a higher financial toll.”

“So far we’re contending with the hackers and criminals and those that want to exploit us, and we’re not being attacked by someone who wants to destroy us,” he said. But, the next financial catastrophe could well be launched by “a group that would want to destroy something.”

He said the federal government needs to produce a digital defense response infrastructure that would include involvement of communications companies, financial companies, energy companies and the best experts in both industry and government.

This would require a modern equivalent of the Goldwater-Nichols Department of Defense Reorganization Act of 1986, which reworked the command structure of the United States military, he said.

In emergencies, this team would gather in a secure Situation Room, map out defenses or responses, then return to their own organizations to implement those responses.