Regulating IT Sector Questioned

August 12, 2009 - Eric Chabrow

When I spoke to Gartner Fellow Richard Hunter the other day for one of our podcast interviews - Feds Seen Regulating IT Industry - his forecast of what future IT sector regulation would be like sounded eerily familiar.

> **If the government sets prescriptive security standards, all security will be similar and new attacks will be more virulent.**

Hunter and his colleagues at the IT advisory firm believe the federal government will be regulating the IT industry by the middle of the next decade industry, as it does the airlines, automotive, financial services, pharmaceutical and telecommunications sectors. In describing an example of regulation, Hunter cited tiered pricing plans for commercial off-the-shelf (COTS) software products based on features offered. His descriptions sound much like a free-market approach to pricing of IT wares forward by Jim Harper, director of information policy studies at the Cato Institute, a libertarian think tank.

Harper believes the federal government can influence pricing and quality of COTS products in the marketplace, without regulations, by establishing standards for products it purchases, agreeing to pay more for greater guarantees of security and suitability. "The government can insist on such contracts, and as a large player in the technology ecosystem it could influence things positively," Harper said in an e-mail message. "Shifting the risk of loss to sellers of technology especially would be an important step toward maturity in technology markets."

Though the Gartner fellow didn't offer his opinion on the merits or IT industry regulation, the Cato director wasn't shy in suggesting such a move could prove perilous. Among those dangers, according to his e-mail:

1) Bad Security: The government doesn't know how to do cybersecurity any better than anyone else. And instead of working on innovations that advance security by leaps and bounds, industry might stop at the level set by government standards.

2) Bad Security II: Monoculture. If the government sets prescriptive security standards, all security will be similar and new attacks will be more virulent.

3) Companies Use Regulation to Hide From Liability: It's easy to envision the biggest technology players feign opposition to regulation, then turn on a dime to embrace it. They might use it to get state laws preempted and avoid liability for negligence or liability under contract theories.

4) Companies Use Regulation to Thwart Competitors: Likewise, companies might embrace regulation to make it more difficult for smaller competitors to meet the government standards that were written for (or by) them.

Despite Harper's cautions, if vendors fail to provide assurances of security and suitability for their products Hunter's predictions of a regulated IT industry will likely transpire.

Click here to listen to a podcast interview with Harper entitled **Can Cyber Terrorism Exist?**

Close Window

GovInfoSecurity.com is your source for government information security news, regulations, and education.