InformationWeek

NSA Surveillance Fallout Costs IT Industry Billions

By Mathew J. Schwartz

November 27, 2013

Creating a massive digital dragnet designed to help U.S. intelligence agencies spot terrorists before they can strike might sound great in the abstract. But what are the real-world implications?

For US technology firms that sell hardware, software, and services, that would be a collective loss of $22 billion to $35 billion through 2016 due to foreign businesses and governments worrying if the National Security Agency (NSA) can spy on those products or services. That figure comes via the Information Technology & Innovation Foundation (ITIF), a Washington-based policy research group backed by many leading technology firms, including Cisco, Google, IBM, and Intel.

"The potential fallout is pretty huge given how much our economy depends on the information economy for its growth," Rebecca MacKinnon, a senior fellow at Washington-based policy group New America Foundation, told Bloomberg. "It's increasingly where the U.S. advantage lies."

But by other analysts' reckoning, however, the ITIF's estimate is too low. Forrester, for example, recently estimated that losses for cloud businesses -- that market is lead by HP, Cisco Systems, and Microsoft -- and managed service providers (MSPs) would total $180 billion through 2016. For comparison's sake, that would be equivalent to about 25% of the annual US defense budget, including spending on the Iraq and Afghanistan wars. Furthermore, Forrester estimated that cloud providers and MSPs might see their revenues decline by 20% over the next three years.

"If a foreign enemy was doing this much damage to the economy, people would be in the streets with pitchforks," Sen. Ron Wyden (D-Ore.) said last month at a Cato Institute conference, The Washington Times reported. Likewise, Rep. James Sensenbrenner (R-Wis.), who authored the Patriot Act, which the White House said authorizes the NSA's digital dragnet, has accused the intelligence agency of overreaching. Some critics, however, have asked why Congressional oversight mechanisms failed to rein in the NSA's surveillance programs.

Still, don't blame just Congress, the White House, or the NSA for the expected business fallout, Forrester analyst James Staten said earlier this year in a blog post. "It's naive and dangerous to think that the NSA's actions are unique. Nearly every developed nation on the planet has a similar intelligence arm which isn't as forthcoming about its procedures for requesting and gaining access to service provider -- and ultimately corporate -- data," he said. For example, Germany's G10 act empowers that country's intelligence agencies to "monitor telecommunications traffic without a court order," he said.

Many technology firms say they've already seen the NSA surveillance scandal start to hit their bottom line. For example, Cisco, which is the world's largest networking equipment manufacturer, recently blamed the NSA revelations for causing buying hesitation in some emerging markets. While Cisco said it had seen only "nominal" concern over the NSA in many countries, it did see a 12% decline in sales in emerging markets, with Chinese buyers, especially, becoming more wary. "It's not having a material impact, but it's certainly causing people to stop and then rethink decisions, and that is reflected in our results," said Robert Lloyd, Cisco's president of development and sales, during a Nov. 13 conference call that reported good earnings, but a bad outlook.

That same day, Richard Salgado, Google's director of law enforcement and information security, warned the Senate Judiciary Subcommittee on Privacy, Technology, and the Law that the NSA's spying activities had caused governments in some countries -- including Brazil and Norway -- to rethink how they'll procure cloud services or work with US firms. Brazil, for example, has introduced a bill that would require service providers such as Google to store all Brazilian data in the country or risk massive fines.

Salgado, in his testimony, said those types of efforts could undermine today's Internet. "If data localization and other efforts are successful, then what we will face is the effective Balkanization of the Internet and the creation of a 'splinternet' broken up into smaller national and regional pieces with barriers around each of the splintered Internets to replace the global Internet we know today," he said.

The use of cloud technology is booming, often offering the only way to meet customers', employees' and partners' rapidly rising requirements. But IT pros are rightly nervous about a lack of visibility into the security of data in the cloud. In this Dark Reading report, Integrating Vulnerability Management Into The Application Development Process, we put the risk in context and offer recommendations for products and practices that can increase insight -- and enterprise security.