

## Don't regulate cyber security

**S**hould the government increase cyber security regulations for private firms? That question was debated recently at the RSA Security Conference in San Francisco. Former White House security advisor Richard Clarke and cryptography expert Bruce Schneier both spoke in favor of increased regulation. But the economics of cyber security and the industry's track record should make us skeptical that government regulation can improve security without damaging innovation.

Many observers believe there is a market failure in cyber security because firms release products with security flaws or because viruses and other cyber attacks cause economic damages. Certainly, these damages are large — the infamous Love Bug virus of 2000 cost the global economy \$2.62 billion, according to the consulting firm Computer Economics.

But cyber security also has costs, and it is possible to buy too much of it, just as it is possible to buy too many padlocks or burglar alarms. The economically efficient level of security requires weighing the potential benefits against the costs.

As long as the benefits and costs of cyber security are internal to firms and their customers, meaning they do not spill over to third parties, the market will provide the efficient level of security. Schneier assumed regulation was necessary when he complained that software makers do not have an economic incentive to improve their product since they do not take responsibility for flaws.

But customers demand products that have new features, are fast, and come to the market quickly. They also demand some level of security in the products, but these demands are weighed against the fact they would increase costs and delay product release. If customers demand greater security in products, software developers who provide it will win out in the marketplace.

The greater challenge is for the market to provide efficient cyber security when some of the benefits spill over to non-customers, but even here the market often does well.

The financial services industry is one that is interconnected and often assumed to be part of the nation's critical infrastructure where the benefits of one firm's security may spill over to others. If there is a market failure in cyber security in the financial industry, we should find low levels of security provision and not find firms increasing security ef-

forts. But the financial services industry shows no evidence of a market failure.

According to the latest Deloitte Global Security Survey, the largest financial, banking, and insurance firms — especially U.S. firms — are employing a wide array of technologies, increasing budgets and staffing to improve cyber security. All firms employed anti-virus software, over 85 percent also used intrusion detection and prevention software, and most firms were experimenting with using many more advanced technologies.

If the spill-over benefits were great and the private returns didn't justify this level of security, we would expect security investment to decline. However, from 2003 to 2004, 63 percent of firms surveyed saw their security budgets increase while only 10 percent decreased, and nearly half of all firms increased security staffing.

Although there does not appear to be a massive market failure in the provision of cyber security in the financial services industry, the introduction of government regulation would create the potential for government failure.

As Harris Miller, president of the Information Technology Association of America, pointed out at the recent conference, "Regulation often becomes the enemy of innovation." A governmental bureaucracy is almost surely going to be too slow and cumbersome to keep up with a field that changes as rapidly as information technology. Regulators are also likely to err in the direction of requiring too much security for fear of a public relations disaster. While firms also fear PR disasters, they are disciplined by profit and loss when they are overly pessimistic. Regulators face no such restraint.

Cyber security has benefits that must be weighed against costs. Reforms should be limited to examining negligence liability standards in situations where security breaches spill over to firms without contractual relations. Direct government regulation will raise costs against consumer wishes, delaying and limiting new products from coming to market. Market forces are better regulators of cyber security than government bureaucrats.

### SECOND OPINION

BENJAMIN  
POWELL

**BENJAMIN POWELL** is the director of the Center on Entrepreneurial Innovation at the Independent Institute, an Oakland, Calif.-based public policy think-tank, and an assistant professor of economics at San Jose State University in California.