CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

COMMENTARY

Innovation and Cybersecurity Regulation

James A. Lewis
Center for Strategic and International Studies
March 2009

The market has failed to secure cyberspace. A ten-year experiment in faith-based cybersecurity has proven this beyond question. The market has failed and the failure of U.S. policies to recognize this explains why we are in crisis. The former chairman of the Security and Exchange Commission, Christopher Cox, a longtime proponent of deregulation, provided a useful summary of the issue when he said, "The last six months have made it abundantly clear that voluntary regulation does not work."

A new Federal approach to cybersecurity will fail if it does not elicit actions that the private sector will not otherwise perform. Government intervention in response to market failure can include regulation (or the threat of regulation) or subsidy. Both have limitations, but both are preferable to inaction. We are at the end of a long era of deregulation, an effort that was initially beneficial but it went too far in the last Administration. Finding a new and more balanced approach will not be easy. The intellectual heritage of deregulation lives in assertions such as any regulation to improve security will hurt innovation. Like all lobbyist mantras, it contains a grain of truth while being fundamentally and dangerously wrong. Innovation is a complex process, and simple statements about cause and effect deserve only skepticism.

Regulation can be an obstacle to innovation when it mandates certain technologies or when it forbids certain activities (it is an instructive contrast that many who oppose cybersecurity regulation do not similarly object to the Digital Millennium Copyright Act, a business inspired law that inhibits security research). Overly prescriptive regulation – such as a requirement to use the DES encryption standard in digital signatures - can block experimentation. But the complete lack of regulation since the start of the commercial internet has not produced the wave of innovation in security we have been promised and we should not expect a continued absence of regulation to have any different result.

This is a more than a drafting problem, although careful regulatory drafting can avoid risk to innovation. Our approach to regulation as a nation is to write authoritative texts that spell out in comprehensive and exhaustive detail what can or cannot be done. This provides certainty, but at the cost of judgement and flexibility. The Federal tax code is an example of the rule-based approach - long and complex, it has inspired innovation, but not the kind that anyone would want. The draft European constitution is another example - it is more than in 100 pages long and spells out in extensive detail various rights, obligations and ceremonies. The contrast is the American constitution, which in a few pages lays out the goals and principles to guide the republic and a process to exercise judgement in the application of those principles. It is worth noting that one constitution has endured for centuries while the other struggles to gain popular approval. The contrast provides a useful guide on how to regulate - describe goals and outcomes, assign responsibilities, and create processes to ensure compliance and resolve disputes.

Regulation and innovation are not inherently at odds. If one extreme – over-regulation - damages the public interest, so does its opposite, a lack of Federal intervention to advance the common interest. Whether this is financial activity, food safety, or automobiles, there are many examples where the Federal government imposed rules and mandated action by the private sector to secure the public, dating back to the early 19th century. One lesson to draw from this experience is that regulation can inspire innovation, by creating demand for new and safer products and by encouraging innovators to work in a conceptual framework that does not make security and safety a tertiary concern.

Regulation can inspire innovation to supply a public good. Regulation creates markets for safety. The first Federal safety regulations, for steamboats after a series of tragedies caused by boiler explosions, led manufacturers to develop safer engines. The requirement to make safe passenger airplanes has not stifled aircraft innovation. The automobile industry resisted innovations like seat belts and safety glass, but now auto companies compete to make safer cars and have found safety to be a useful marketing tool. Not coincidently, traffic fatalities have declined, something that would not have happened otherwise. A decision not to regulate would have slowed or stopped innovation in automobile safety. Without regulatory effort, we as a nation will not get innovation in cybersecurity at anywhere near adequate levels.

A related objection notes that regulated industries are not secure. This does not mean that regulation is ineffective for improving security. The regulations could be inadequate - a reasonable assumption given the ideological predilection of the previous administration. Or cybersecurity could be low priority as a regulatory goal - also a reasonable assumption given the general inattention to cybersecurity. Or it could reflect the inability of a regulated industry to secure itself when the larger cyber environment is insecure - regulation could be well designed and implemented, but weaknesses in international law enforcement, deterrence, and the regulation of other connected sectors would undermine effectiveness. The unasked question is whether regulated industries are more secure than they would have been otherwise – banks still suffer losses but their losses would be much more severe if they had not been forced by regulators to improve security. A partial improvement is better than no improvement, and we want to avoid a situation where the absence of a perfect answer becomes an excuse for inaction.

Judging from the evidence, the most likely cause is that cybersecurity has never been a priority for regulatory agencies. Agencies lack the interest and expertise to advance cybersecurity, and they have regarded it as peripheral to their mission. A 2008 GAO study found that there is essentially no cyber regulation now outside of the financial sector. This reflects a limited understanding of the centrality of cyberspace and digital technologies to the economic performance and national security of the United States.

A regulatory agenda for cybersecurity does not mean immense new regulation, like HIPAA or Sarbanes Oxley, based on an all- encompassing law and prescribing action in excruciating detail. Instead, a new approach should begin by coordinating action among existing regulatory agencies (there is no coordination now), making cybersecurity a priority mission for them (it is currently not even a secondary concern) and establishing common performance baselines and metrics for an acceptable level of security. In some instances, new authorities may be required. The most important step is to make cybersecurity a priority for regulatory agencies and ensure that their agendas for action include securing networks and ensuring the delivery of reliable and safe services to the public. Both law and regulation

are still backwards facing, looking to the 1980s, when a computer was optional equipment, as if we could somehow go back to faxes and photocopiers for business.

Digital networks form the backbone of our economy, but they are easily and illegally accessed by our foreign competitors and opponents. The primary damage to U.S. national security and economic strength from poor cybersecurity comes from the theft of intellectual property and the loss of advanced commercial and military technology to foreign competitors. A failure to secure America's information infrastructure weakens the United States and makes our competitors stronger. Weak cybersecurity means that when we innovate, our competitors share the benefits of our investments at no cost, while freeing up their own resources for innovation in other areas.

One national goal should be to enable innovation. The United States will benefit from positioning itself to remain a leader in creating new services and technologies. This requires making the larger business climate amenable to change and enabling entrepreneurs and innovators to make new goods and services. There are many obstacles to innovation – the credit crisis, the use of law and regulation by incumbents to defend business models and block change, inflexible labor and health care rules, and years of underinvestment in human capital and research - but cybersecurity regulations are not among them.