The Private Sector: A Reluctant Partner in Cybersecurity

It may seem obvious that the private sector should be keen to protect its computers and networks from cyber attacks by criminals and foreign agents. After all, hacking has caused considerable losses of trade secrets and other proprietary information. Moreover, evidence suggests that cyber attacks can take a kinetic form, which can harm the equipment and facilities—such as the national electrical grid—of those attacked. However, as will be seen shortly, the private sector is far from rushing to protect itself from such attacks. The reasons for this reluctance range from the understandably pragmatic to the ideological. Meanwhile, in spite of major implications of this reluctance for homeland security, both the Bush and the Obama administrations limited themselves to cajoling the private sector to embrace much stronger cybersecurity measures rather than mandating their introduction.

A. Threat Levels

Private sector firms suffer considerable damage from cybersecurity breaches. A report from the Center for Strategic and International Studies finds that the costs to the global economy—which encompass losses of intellectual property, outright cybercrime, unauthorized access to confidential business and stock information, the costs of recovering from cyber attacks, and the value of reputational damages—of malicious cyber activity are “probably . . . [as much as] $400 billion”—or even $1 trillion per year. The United States alone is estimated to suffer up to $120 billion in economic losses per year.¹ In 2012, one metallurgical corporation reportedly “lost technology to China’s hackers that cost $1 billion and 20 years to develop.”² In some cases, companies have been driven entirely out of business by Chinese hackers’ persistent cyber espionage.³
One report estimates that 508,000 American jobs have been lost due to cyber crime. General Keith Alexander, until recently the director of the National Security Administration and commander of the U.S. Cyber Command, has estimated that economic espionage, including the kind practiced by Chinese and Russian hackers, represents “the greatest transfer of wealth in history.”

No industry is immune: cybersecurity firm Mandiant estimated in 2006 that cyber attacks tied to China’s People’s Liberation Army (PLA) alone targeted twenty separate, major industries including telecommunications, energy, and aerospace. Even Google—arguably one of the most sophisticated companies in the world with regard to computer networks—fell victim to a complex hack that originated in China, during which the hackers “appropriated some of Google’s search engine source codes, a vital piece of intellectual property.”

These estimates of losses do not include the legal costs of data breaches and those resulting from consumer confidence; moreover, companies are often forced to pay fines when their cybersecurity measures fail to protect consumer information. Heartland Payment Systems, for example, was slapped with $150 million in fines and legal costs that stemmed from a 2007 cybersecurity breach in which more than 100 million credit and debit card numbers were illegally obtained by hackers. One research institute estimated that malicious attacks cost American firms $277 per customer or user whose information was put in jeopardy by a company’s cybersecurity failures. Nevertheless, many corporations resist introducing many of the cybersecurity measures recommended by the U.S. government.

B. Reasons for Weak Private Sector Response

The private sector’s reluctance to adopt strong cybersecurity measures is driven by a combination of principles and practical concerns. Four of the most frequently articulated arguments against government mandated private sector cybersecurity standards follow.

First, significant segments of the private sector consider proposed requirements to introduce cybersecurity measures to be an additional form of government regulation. The Business Software Alliance opposes placing “undue regulatory burdens on industry,” and the U.S. Chamber of Commerce opposes “legislation establishing regulatory-based cybersecurity standards.” The Heritage Foundation opposed the same bill because it would “create a cumbersome regulatory process.” These and other corporate leaders and economically conservative commentators adhere to the laissez-faire and libertarian principles that private enterprise has a right