AMITAI ETZIONI

Cybersecurity in the Private Sector

The nation's businesses manage a significant share of online activity related to national security and must play a larger role in ensuring the overall integrity of the system.

The United States is facing major cyber attacks by criminals and agents of foreign governments, with attacks penetrating the military establishment and the private sector alike. The need to better protect military systems is well recognized. But protecting the private sector has drawn less attention, and even some resistance. Yet protecting the private sector is increasingly critical, because the United States, more than most if not all other nations, draws heavily on private corporations for ensuring national security. Corporations manufacture most of the nation's arms. Corporations produce most of the software and hardware for the computers the government uses. And corporations, under contract with the government, carry out many critical security functions, including the collection and processing of intelligence and the conduct of covert operations.

The heavy reliance on the private sector for security, including cybersecurity, was accentuated during the Bush administration, which contracted out significant parts of missions that previously were carried out in-house. This trend has been only slightly scaled back during the Obama administration. In short, it is now almost impossible to imagine a secure United States in which security is provided only to the computers and Internet used by the public sector.

At first blush, it might seem that the private sector would strongly support new measures that enhance cybersecurity. Many of the crimes committed in cyberspace, such as electronic monetary theft, impose considerable costs on private companies. The same holds for industrial espionage, especially from other countries, which deprives U.S. corporations of the fruits of long investments in R&D and grants major advantages to unfair competitors. In addition, if cyber warfare were to break out, many of the assets that would probably be damaged belong to private corporations. And not to be overlooked, businesses are operated by individuals who, one assumes, have a vested interest in the nation's security.

Businesses, however, have not displayed a strong commitment to cybersecurity, to put it mildly. One reason is philosophical. Many corporate leaders, and the think tanks that are associated with the corporate world, maintain one version or another of a libertarian or conservative laissez-faire approach, basically holding that they are best left alone, not regulated, free to follow their own courses. They further hold that their main duty is to their shareholders, who own the corporations, and not to the common good.

In addition to such philosophical arguments, however, there are a number of more practical barriers that have limited, and continue to limit, efforts to improve private-sector security.

Missing ingredients

Some security experts argue that current incentives for corporations to better secure their computer systems are not aligned in ways that promote voluntarily actions. The credit card system is often cited as an example where incentives are correctly aligned, dating from the 1970s when the government placed limitations on consumer liability for fraudulent charges. This change in liability motivated the industry to develop needed security measures.

No such realignment has occurred in cyberspace, however. Despite the rapid rise of Internet bank theft, for example, companies often deem the costs of adding security measures to be higher than the losses from cyber theft. Also, the effects of industrial espionage are often not in evidence for several years, beyond the horizons of many CEOs who are concerned primarily with the short-term profits and stock prices of their corporations. In order to prevent what corporate officials call "negative publicity or shareholder response," companies regularly have absorbed losses incurred by security breaches rather than reveal weaknesses in cybersecurity systems, all in the name of protecting reputations and shareholder values.

Fred H. Cate, the director of the Center for Applied Cybersecurity Research at Indiana University and a member of a number of government-appointed information-security advisory boards, has pointed out that cybersecurity is desperately in need of better incentives. According to Cate: "Although it's often preferable to let markets create appropriate incentives for desired behaviors, in some instances, government intervention is necessary. Information security is one of those instances. The threats are too broad, the actors too numerous, the knowledge levels too unequal, the risks too easy to avoid internalizing, the free-rider problem too prevalent, and the stakes too great to believe that markets alone will be adequate to create the right incentives or outcomes."

Other experts point to a need for increased regulatory control, done wisely. Phillip Bond, president and CEO of TechAmerica, a technology industry association, has said that "it is crucial that Congress act and pass national legislation addressing security and data breach." Black Hat, an international conference series of experts on information security, advocates for an approach called "smart regulation," which articulates an end state and allows the regulated to figure out how best to get to it.

Providing cybersecurity via regulations, however, has encountered resistance by many private-sector representatives who hold that forcing companies to comply will harm their flexibility and ability to innovate. Further, businesses consider it unfair and inappropriate to demand a task of private industry—securing critical national assets—that is essentially a public-sector responsibility. Some in the private sector regard security requirements imposed by the government as unfunded mandates, as a form of taking, and demand that the government cover the costs involved. Still others believe that the government might be exaggerating the cybersecurity threats.

For such reasons, corporations have been slow to act, and may be slowing even more. For example, according to Lieberman Software's 2009 survey of information-technology (IT) executives in the private sector, the limited cybersecurity measures that corporations have created have been largely motivated by cost savings, with minimal concern for the protection of information. The survey also found that the majority of private-sector IT budgets are decreasing, with many corporate employees citing the financial effects of the recession.

Costs of inaction

The bottom line is that incentives have not been changed much, few regulations have been enacted, and no major public funds for private security have been made available. The net result is that cybersecurity is weak for work carried out in and by the private sector, and public security is paying the price.

The costs can be seen in the major security breaches in recent years, including at major defense contractors such as General Dynamics, Boeing, Raytheon, and Northrop Grumman. Examples include a theft in which top-secret plans for the F-35 Joint Strike Fighter were stolen by hackers, presumed to be Chinese. According to the report of the House of Representatives' Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, known widely as the Cox Commission report, "has stolen classified information on all of the ' most advanced thermonuclear warheads, and several of the associated reentry vehicles."

Indeed, China often comes under suspicion. Richard Clarke, who served as special adviser to the White House on cybersecurity during the early 2000s, reported in his 2010 book *Cyber War: The Next Threat to National Security and What to Do About It*, that Chinese hackers targeting U.S. corporations have stolen "secrets behind everything from pharmaceutical formulas to bioengineering designs, to nanotechnology, to weapons systems, to everyday industrial products."

The defense establishment also has fallen victim to a number of high-profile instances of cyber espionage. In 2008, foreign intruders managed to break into the secure computers of the U.S. Central Command, which oversees the wars in and . William J. Lynn, deputy secretary of Defense, described the attack as "a network administrator's worst fear" and "the most significant breach of U.S. military computers ever." And in 2007, unknown attackers, probably working for a foreign government, stole several terabytes of information from the Departments of Defense and State. The amount stolen was nearly equal to the amount of information in the Library of Congress.

Clearly, the military's own computers—produced by the private sector, run on software from the private sector, and often maintained and serviced by the private sector—are not well protected. The networks of the Department of Homeland Security (DHS) also are poorly protected. In a typical incident, a private firm that was contracted in 2007 to build, secure, and manage DHS networks failed to properly complete the job, and for months DHS was left unaware as hackers, probably based in China, stole information from its computers.

Richard Clarke described another revealing instance in his book. Before the 1990s, the Pentagon relied primarily on expensive, but highly secure, specialized software designed by in-house programmers and a few select defense contractors. However, Microsoft, a major donor to both political parties since 1998, convinced government officials that in order to reduce costs and improve interoperability, the military should use off-the-shelf commercial software, particularly Microsoft software. The transition to Microsoft's software, some of it manufactured in , greatly weakened the security of the military computers. Moreover, in one telling incident, the *U.S.S. Yorktown*, a Ticonderoga-class cruiser, became inoperable after the Windows NT system administering its computers crashed.

After this and what Clarke called a "legion of other failures of Windows-based systems," the Pentagon considered a shift to free, open-source operating systems, such as Linux. The code of open-source software can be adapted by the user, and so the government would be free to tailor the system to the particular security needs of various agencies. Microsoft has refused to allow many federal agencies and corporations to view or edit its source code, thereby limiting agencies' ability to fix security flaws and system vulnerabilities. However, a switch to Linux would have greatly reduced Microsoft's business with the government. The company was already fiercely opposed to regulation of its products' security features. Microsoft "went on the warpath," pouring money into lobbying Congress against regulations, Clarke recalled, adding that "Microsoft's software is still being bought by most federal agencies, even though Linux is free."

James Lewis, a cybersecurity expert at the Center for Strategic & International Studies, has summed up the situation by declaring that the nation's digital networks are "easily" accessed by foreigners, both competitors and opponents. In a report titled *Innovation and Cybersecurity Regulation*, published by the center in 2009, Lewis flatly stated that "the market has failed to secure cyberspace. A ten-year experiment in faith-based cybersecurity has proven this beyond question."

The government is not scoring much better. As Richard Clarke has asked, "Now, who's defending us? Who's defending those pipelines and the railroads and the banks? The Obama administration's answer is pretty much, 'You're on your own,' that Cyber Command will defend our military, Homeland Security will someday have the capability to defend the rest of the civilian government—it doesn't today—but everybody else will have to do their own defense. That is a formula that will not work in the face of sophisticated threats."

Government resistance

During his tenure at the White House, Clarke attempted to implement an ambitious regulatory regime, but his plan was largely blocked by antiregulation forces within the administration of George W. Bush. According to Stewart A. Baker, who served as first assistant secretary of homeland security for policy at the time, the proposed strategy "sidled up toward new mandates for industry," would have required the formation of a security research fund that would draw on contributions from technology companies, and would have increased pressure on Internet companies to provide security technology with their products. These requirements were viewed as too onerous for business by many within the administration, and ultimately "anything that could offend industry, anything that hinted at government mandates, was stripped out," Baker recalled.

Companies regularly have absorbed losses incurred by security breaches rather than reveal weaknesses in cybersecurity systems, all in the name of protecting reputations and shareholder values.

Many corporations shy away from cybersecurity responsibility. As Terry Zink, program manager for Microsoft Forefront Online Security, has pointed out, Internet service providers (ISPs) and individual users "don't have the expertise or financial motivation required to do it. Government can recruit bright individuals to create a program of cyber-health monitoring and they have access to the resources necessary to implement such a program. ...And let's face it, government doesn't *have* to have a profit motive to support something. The government supports *lots* of programs that otherwise lose money in the name of the public good."

Moreover, it is unclear who is responsible for maintaining the security of many critical assets. Currently, DHS is working to secure the ".gov" domain, but not critical infrastructure. As President Obama stated in 2009 when unveiling his administration's cybersecurity policy review, "Let me be very clear: My administration will not dictate security standards for private companies." This is a statement of considerable import, given that many of the missions carried out in other nations by the military (or by companies owned and managed by the state) are carried out in the by the private sector. It might be argued that the president merely said he will not "dictate" which security standards must be followed but will find some other ways of making or persuading the private sector to adhere to these standards. However, the president did not declare or follow such a course, keeping instead within the custom of previous administrations.

Modest proposals

Several commissions have studied what must be done to enhance cybersecurity in cooperation with the private sector. Their reports tend to follow the optimal design approach: They list what ought to be done in a world free from ideological biases and political capture, and thus read like the plans of someone who is designing a building to be erected on a heretofore empty lot. Moreover, the reports typically do not examine the costs of the recommended measures, as if there were no difficulties in attaining public funds or imposing costs on the private sector. It is hence not surprising that the recommendations have been largely ignored, although after considerable delay the government did create a Cyber Command within the U.S. Strategic Command.

Even rather elementary cybersecurity measures have not been introduced. To provide but one example, Richard Clarke, recognizing the limits of what can be done, argued for at least one low-cost, high-yield measure: introducing filters at the major "backbone" Internet service providers, run by the biggest private Internet companies, where nearly all Internet traffic passes through at one point or another. Filters could be set on the main ISPs to scan for malware and cyber attacks with no noticeable delay in the speed of Web surfing. This would help secure the vast majority of information transmitted on the Internet. But business interests and privacy concerns made the idea controversial and prevented its implementation. Finally, in May 2011, two and a half years into the Obama administration, after new cyber attacks that penetrated the personal accounts of numerous public officials, the National Security Agency began to work with ISPs on a program—on a trial basis and with voluntary participation—to protect the from such attacks.

Another needed measure calls for separating critical infrastructure, such as the electrical grid, from the Internet. This is a basic security measure that would significantly enhance the nation's protection against potential cyber threats without exacting high financial costs, or any privacy costs. Clarke argued that such a step has not been taken because it cannot be done without additional federal regulation, which butts up against the stance of industry officials that they should be left largely unregulated with regard to cybersecurity. Corporations have taken this stand despite the fact that cybersecurity experts have easily been able to access power grid controls from public Internet sites.

Indeed, federal policy is currently moving in the opposite direction, toward greater connectivity for the nation's energy grid. The "smart grid" initiative advanced by President Obama is designed, in the administration's view, to save money and update an aging energy grid by integrating various power suppliers into one system by using a digital network. But research shows that a smart grid will introduce new problems, such as increasing the vulnerability to cyber attack as power grid resources become increasingly linked to the Internet.

The could significantly enhance its protection from cyber threats by working toward greater security for computer-component supply chains. The individuals who led the Obama administration's cybersecurity review—Jack Goldsmith, a former assistant attorney general, and Melissa Hathaway, a cybersecurity expert—warned of the "excessive security vulnerabilities" that result from "the use of commercial off-the-shelf software produced in a global supply chain in which malicious code can be embedded by stealth." However, the government is continuing to use generic software and hardware, including some produced overseas.

Needed actions

After major online breaches in 2011 into the CIA, the U.S. Senate, and the International Monetary Fund, among many others, the Obama administration unveiled several proposals to enhance cyber security. In May 2011, it presented a proposal that seeks to knit together a "security infrastructure" to encompass the public and private sectors, with actions proposed at the state, federal, and international levels.

The plan features a new national data-breach reporting policy that would require private institutions to report security breaches to the affected individuals and the Federal Trade Commission (FTC) within 60 days. (This, presumably, would create an incentive to fix security lapses that is lacking when customers are not informed). The FTC would be responsible for enforcing penalties against violators, and DHS would have a regulatory role over the cybersecurity of critical infrastructure, which would include defense firms and major telecommunication and banking institutions. The plan also seeks to introduce mandatory minimum sentences for cyber criminals. On the international level, the proposal resolved to work with "like-minded states" to create an international standard for cyber security.

The proposal has encountered some resistance from the private sector. Larry Clinton, president of the Internet Security Alliance, told a House Homeland Security panel studying the plan that it creates "counter-incentives" by requiring businesses to publicly disclose their security statuses, argued that if corporations feel they may be "named and shamed for finding [security breaches], we've created exactly the wrong incentives." It should be noted, however, that the proposal would protect companies from liability if they voluntarily share threat information with DHS for cyber investigations. The libertarian response can be summed up by the headline of an article in the August/September 2011 issue of *Reason* magazine: "The Cybersecurity-Industrial Complex: The feds erect a bureaucracy to combat a questionable threat."

Republicans intend to formally respond to the proposed plan in October 2011, after deliberations by a party taskforce in the House. But the proposal already has been met with concerns about "regulation for regulation's sake," as Representative Bob Goodlatte (R-VA) put it. The plan has found some measured support from Senator Susan Collins (R-ME), who has worked extensively on the issue alongside Senators Joseph Lieberman (I-CT) and Tom Carper (D-DE). Indeed, there is at least hope that security threats can foster bipartisan cooperation, as happened when Senators John McCain (R-AZ) and John Kerry (D-MA) joined forces to support U.S. actions as part of the interventional intervention in Libya.

Given the escalating cyber threats and a reinvigorated White House drive, cybersecurity may now gain more attention. However, increased attention—or, even better, firm government action—is far from a secure bet.

Recommended reading

Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010).

James Lewis, *Innovation and Cybersecurity Regulation* (Washington, DC: Center for Strategic and International Studies, March 2009); http://csis.org/files/media/csis/pubs/090327_lewis_innovation_cybersecurity.pdf.

Amitai Etzioni (etzioni@gwu.edu) is a University Professor and director of the Institute for Communitarian Policy Studies at The George Washington University. He is the author of Security First: For a Muscular, Moral Foreign Policy and The Limits of Privacy.