Number 13-3

NIST Economic Analysis Office
Economic & Policy Analysis Brief

The Economic Benefits from Improved Cyber Security Infrastructure

Gary Anderson (gary.anderson@nist.gov)

Gregory Tassey (gtassey@nist.gov)

Key Findings:

- *Cyber Security Infrastructure gaps cost industry $6 billion*
- *Improved cloud security, improved mobile device security and improved security metrics offer the greatest economic benefit*

Leading government officials have warned that a "cyber 9/11" could happen at any time. A coordinated terrorist cyber attack on a massive scale could potentially shut down the domestic economy. Even without such a pervasive assault, banks, utilities, and critical infrastructure industries are under constant attacks from nation states and other groups. It is no longer a matter of if power grids, telecommunications networks, chemical plants, large banks, water supplies, and other critical infrastructure will be attacked, but rather when will the next one occur and who will be the target. Cyber security threats and attacks cost U.S. companies tens of billions of dollars a year in direct costs—spending cyber security technologies and activities—and much more in indirect costs, including the loss of intellectual property, service or product quality degradations, and reputational or customer loss. Cyber criminals target individuals and corporations with more frequent, more sophisticated, and more coordinated assaults.[1] General

[1] For example, the IRS reported that 938,664 tax returns totaling $6.5 billion in fraudulent refunds were identified in processing year 2011 (TIGTA 2012). Approximately 80% of returns have been filed online in the 2012 tax season, suggesting that electronic identity theft is likely a very significant mode of conducting fraud. Internal Revenue Service. (2012) *Filing Season Statistics for Week Ending June 8, 2012(* http://www.irs.gov/uac/Filing-Season-Statistics-for-Week-Ending-June-8,-2012).

Topics Covered by Economic & Policy Analysis Briefs:

- *Economic rationales for government roles*
- *Characterization and measurement of market failures*
- *Economic impact studies*
- *Gap analyses (strategic planning studies)*

Other Briefs:

- *Technology Clusters*
- *Economic Impacts of Technology*
- *Technology-Based Growth Strategies*

Keith Alexander, Chief of the U.S. Cyber Command and Director of the National Security Agency, reports that between 2009 and 2011 the United States saw a 17-fold increase in attacks.[2]

A recent study, commissioned by the National Institute of Standards & Technology (NIST), identified two key economic problems: 1) the public and private sector invest too little in cyber security; and 2) the investments that are made in improved cyber security are excessively costly. Like national defense, cyber defense is a public good and private investment alone will not provide adequate security. Due to the agency's mission NIST focused on the second problem, the economic factors that negatively impact the efficiency of cyber security investment and create the need for technical infrastructure. Cyber security technical infrastructure (CSTI) includes operating protocols, test methods, reference data, performance metrics, analytical tools, and information sharing systems ("infratechnologies"), as well as novel security concepts and precompetitive prototype systems ("technology platforms"). By enabling public and private organizations to detect threats and vulnerabilities as well as measure performance of their investment, this technical infrastructure acts as an "industrial commons" [3] that increases the efficiency and effectiveness of all other cyber security investments The NIST study identifies explicit gaps in CSTI and estimates that these gaps currently cost industry approximately $6.0 billion.[4]

According to the analysis, the highest priority CSTI needs (investment "gaps") across the private sector include the ones in the table below.

Meeting these CSTI needs will enable industry and government stakeholders to measure errors in software, ascertain the quality of software with respect to achieving cyber security, and fully understand the nature of vulnerabilities. CSTI leverages software suppliers' efforts to compete along the critical dimension of quality and increases the effectiveness and efficiency of all stakeholders' production and use of secure cyber environments. The net impact of CSTI is to increase firms' returns on their R&D investments in cyber security and customers' willingness to pay

[2] Sanger, David E. and Eric Schmitt, "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure," *New York Times*, July 26, 2012 (http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html).

[3] See Pisano, Gary P. and Willy C. Shih, "Restoring American competitiveness," *Harvard Business Review,* July 2009.

[4] The $6 billion estimate also can be viewed as a cost to the economy of not expending the extra 10% on CSTI.

Topics Covered by Economic & Policy Analysis Briefs:

- *Economic rationales for government roles*
- *Characterization and measurement of market failures*
- *Economic impact studies*
- *Gap analyses (strategic planning studies)*

Other Briefs:

- *Technology Clusters*
- *Economic Impacts of Technology*
- *Technology-Based Growth Strategies*

for cyber products and services.

Just as conventional economic infrastructure (transportation, communication, etc.) increases the productivity of private-sector investment, CSTI stimulates the development, deployment and diffusion of new cyber security technologies.

CSTI Need	Economic Benefit of Meeting Need ($ million)
Improved Cloud Security	1,146
Improved Mobile Device Security	928
Specification and Collection of Security Metrics	668
Standards for meeting auditing and compliance requirements	658
Automated Threat detection and prevention	633
Increased sharing of threat data	631
Improved education about IT security best practices	585
Improved authentication of system users	562
Tools for protection and mitigation from loss of equipment and media	189
Total	6,000

However, like all infrastructure, CSTI has characteristics that prevent individual firms from capturing the full benefits from investments. In particular, other competing firms cannot be excluded from using it and one firm's use does not preclude another's. Thus, firms that develop technology platforms and infratechnologies on their own are not fully compensated for the investments they make and the associated risks they incur. In other words, CSTI creates spillover benefits enjoyed by all firms participating in the affected markets, so these other firms have a strong incentive to "free ride;" that is, to wait for someone else to incur the cost of developing the CSTI. The resulting underinvestment is especially severe in the early part of a cyber security technology's development and thereby delays the introduction of new products and services requiring higher levels

Topics Covered by Economic & Policy Analysis Briefs:

- *Economic rationales for government roles*
- *Characterization and measurement of market failures*
- *Economic impact studies*
- *Gap analyses (strategic planning studies)*

Other Briefs:

- *Technology Clusters*
- *Economic Impacts of Technology*
- *Technology-Based Growth Strategies*

of cyber security.

Because the use of CSTI by a particular individual or organization does not reduce the value of CSTI to any other organization (a characteristic of all infrastructure) and because, in fact, its value is greatest when openly available and widely used, the profit motive will not provide sufficient incentive to produce CSTI. This "market failure" justifies NIST's mission of developing and fostering adoption of critical and equitable technical infrastructure.

NIST's focus as an organization is to develop infratechnologies and technology platforms that will help U.S. organizations increase productivity and quality, primarily by compensating for barriers to adequate investment. Developing the technical infrastructure that can measure, test, and assure the quality of products between tiers of a supply chain (e.g., software providers and customer organizations) is a vital and traditional NIST role. Information market failures of this type, where products are of unknown quality, critically increase the cost and decrease the effectiveness of all efforts to produce a secure cyber environment.

Beyond the need for additional tools to measure quality, additional market failures affect the development of sufficient CSTI. For example, a coordination market failure slow or even prevents the development of novel technologies such as those that could improve threat detection beyond the current practice of scanning for known and previously implemented threats. Such developments require significant investment in generic platform technologies and also in infratechnologies/standards to ensure that the needed threat data are uniform across software platforms. The private sector is unlikely to invest sufficiently in such CSTI.

In 2012, planned investment in CSTI-related R&D activities by the federal government, cyber security industry consortia, and private firms was estimated to be $716.1 million. The federal government's share was 70.8% of total planned CSTI funding ($506.9 million), followed by private firms at 19.9% ($142.7 million), and industry consortia at 9.3% ($66.5 million). Investment in the CSTI by private-sector organizations is primarily focused on the development of proprietary technologies for internal use, although private-sector organizations also support industry-wide CSTI R&D projects and subsequent adoption through funding provided to and

Topics Covered by Economic & Policy Analysis Briefs:

- *Economic rationales for government roles*
- *Characterization and measurement of market failures*
- *Economic impact studies*
- *Gap analyses (strategic planning studies)*

Other Briefs:

- *Technology Clusters*
- *Economic Impacts of Technology*
- *Technology-Based Growth Strategies*

participation in industry consortia. Labor allocated by the private sector to participation in industry associations and consortia were estimated to be approximately $140 million.

The gaps identified in the NIST study constitute CSTI shortfalls that, if left at their current levels, will continue to inhibit the efficiency of private efforts to produce secure cyber environments. An increase in the CSTI as a result of public investment means that private investments will have a higher rate of return; that is, each dollar invested will result in a greater increase in the level of cyber security than otherwise would have occurred.

The NIST study identified potential CSTI that, if developed and assimilated by industry, could narrow the security gap in each of the nine areas by at least 10%. The economic benefits accruing to the cyber security operations of U.S firms are estimated to be approximately $6.0 billion.[5] The largest estimated benefits would come from improving the CSTI supporting cloud security ($1.1 billion), mobile device security ($928 million), and specification and collection of security metrics ($668 million).[6]

These impact estimates were derived from an analysis of 162 survey responses received from U.S. IT security managers, 72% of which indicated that they were responsible for cyber security for their entire organization.[7] Six industries accounted for 73% of all respondents, ordered by degree of representation: (1) Finance and insurance, (2) Information, (3) Manufacturing, (4) Professional, scientific, and technical services, (5) Health care and social assistance, and (6) Utilities.
On average, respondents indicated a willingness to spend approximately 14.7% of their cyber security budgets to increase their cyber security effectiveness by 10%.[8] A typical company was willing to spend approximately about $1 million to reduce

[5] The $6 billion estimate also can be viewed as a cost to the economy of not expending the extra 10% on CSTI.

[6] Based on interviews with industry, these benefits are estimated to accrue over a 4 year period, with the majority of benefits estimated to accrue in the first two years.

[7] Respondents to the survey completed in early 2012 were asked a series of prospective questions to ascertain their willingness to pay for improvements in the CSTI. Specific survey questions were structured to determine the total benefits organizations would receive if CSTI gaps were narrowed by asking them how much they would be willing to pay for a 10% increase in cyber security effectiveness.

[8] Most organizations who responded to the survey (65%) annually spend less than 5% of their IT budgets on IT security. Only 23% of organizations spend more than 10% on IT security, and 41% spend 1-2% on IT security.

incidents and breaches by 10%.

The NIST study can be accessed at
http://www.nist.gov/director/planning/upload/report13- 1.pdf