Planning Report 13-1

Economic Analysis of an Inadequate Cyber Security Technical Infrastructure

Brent R. Rowe
Igor D. Pokryshevskiy
RTI International
3040 E. Cornwallis Road
Research Triangle Park,
NC 27709

with

Albert N. Link
University of North Carolina
at Greensboro
Douglas S. Reeves
North Carolina State University

February 2013

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

February 2013

Economic Analysis of an Inadequate Cyber Security Technical Infrastructure

Final Report

Prepared for

Economic Analysis Office
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Prepared by

Brent R. Rowe
Igor D. Pokryshevskiy
RTI International
3040 E. Cornwallis Road
Research Triangle Park, NC 27709

with

Albert N. Link
University of North Carolina at Greensboro
Douglas S. Reeves
North Carolina State University

RTI Project Number 0212660

RTI Project Number
0212660

Economic Analysis of an Inadequate Cyber Security Technical Infrastructure

Final Report

February 2013

Prepared for

Economic Analysis Office
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Prepared by

Brent R. Rowe
Igor D. Pokryshevskiy
RTI International
3040 E. Cornwallis Road
Research Triangle Park, NC 27709

with

Albert N. Link
University of North Carolina at Greensboro
Douglas S. Reeves
North Carolina State University

Contents

Appendices

Figures

Number **Page**

Tables

EXECUTIVE SUMMARY

The focus of this study, commissioned by the National Institute of Standards and Technology (NIST), is on one component of cyber security—the cyber security technical infrastructure (CSTI). The CSTI is an example of what is sometimes called an “industrial commons”[1]: the embedded knowledge and technology framework that enhances the efficiency, effectiveness, and productivity of the proprietary capital and labor that use it. It is a common set of technologies, standards, policies, and procedures that competing firms draw on to unify their cyber security assets and achieve a more secure environment.

According to various estimates, cyber security threats and attacks cost U.S. companies tens of billions of dollars a year in direct costs—spending on proactive and reactive cyber security technologies and activities—and likely much more in indirect costs, including the loss of intellectual property, service or product quality degradations, and reputational or customer loss. Although the total magnitude of these costs is unknown, the news media are replete with evidence that attests to the substantial impact inadequate cyber security has on companies and individuals.

General Keith Alexander, Chief of the U.S. Cyber Command and Director of the National Security Agency, points out that the United States saw a 17-fold increase in cyber attacks between 2009 and 2011.[2] In addition, individuals are being targeted by increasingly sophisticated, coordinated attacks to conduct identity theft or to use individuals’ computers to attack others.[3] As described in the White House’s *Strategic Plan for the Federal Cybersecurity Research and Development Program* (2011a), a thorough understanding of cyber security vulnerabilities is needed to treat the causes of cyber security problems.

Although cyber threats cannot be completely prevented, networks can dissuade or fend them off through strong defensive postures. An issue is that the security apparatus protecting networks may itself be an amalgam of solutions assembled over time by successive security personnel. Not only are potential vulnerabilities inherent in software and architecture design; they are also associated with the human element in network implementation, operation, and maintenance.

The CSTI is only one part of cyber security, but an important one that unifies cyber securities assets. This report summarizes the most damaging CSTI inadequacies, or gaps, from

[1] See Pisano and Shih (2009).

[2] See article by Sanger and Schmitt (2012).

[3] For example, the IRS reported that 938,664 tax returns totaling $6.5 billion in fraud 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 (IRS, 2012).

the perspective of U.S. industry’s cyber security directors, and quantifies a first-order approximation of economic benefits of narrowing those gaps.

This study quantifies the economic benefits to firms’ cyber security operations of reducing the number of incidents and breaches by 10% as a result of targeted CSTI research and development. In recent years, multiple studies have aimed to offer some sense of the drag of cyber security problems on the U.S. economy but without offering many specifics as to what the issues are and how those estimates relate to real business issues. In contrast, this study focuses the lens on what cyber security directors believe the problems are and what the tangible economic benefit would be to their operations by improving the effectiveness of the CSTI, and therefore their cyber security, by just 10%.

ES.1 Cyber Security Technical Infrastructure (CSTI)

CSTI components include standards, operating protocols, test methods, reference data, performance metrics, analytical tools, and information sharing systems (collectively referred to as “infratechnologies” [see Table ES-1]), as well as novel security concepts and precompetitive prototype systems (called “technology platforms”) that collectively raise the level of national cyber security.[4] By enabling stakeholders to measure errors in software, ascertain the quality of software regarding cyber security, and fully understand the nature of vulnerabilities, CSTI creates the incentive for software suppliers to compete along the critical dimension of quality and increases the effectiveness and efficiency of all stakeholders’ production of secure cyber environments. The CSTI increases firms’ return on cyber security R&D investments and increases customers’ willingness to pay for products and services. In other words, the CSTI stimulates the deployment and diffusion of new technologies.

If the CSTI raises the collective cyber security level, then it follows that CSTI gaps represent weaknesses that lower cyber security. Using an armor metaphor, if cyber security is a shield protecting network assets, security software and hardware systems would be the shield’s plates, which are held together by bindings—the CSTI. Irrespective of how strong the plates are, gaps in the bindings allow attacks to go through.

[4] The CSTI supports an organization’s ability to efficiently detect threats, and provides some level of assurance that its systems adhere to best practice. For example, the CSTI supports the communication of threats by establishing a protocol that network operators follow to assess, measure, and communicate those threats. The CSTI does not include the central server operations of any one firm, nor does it include the workforce assigned to monitor, detect, and investigate intrusions. The distinction between the CSTI and physical assets is important because in common IT-industry parlance, technical infrastructure refers to physical assets such as servers, desktops, cabling, and software systems.

Table ES-1. Examples of Cyber Security Infratechnologies

Type	Description	CSTI Examples
Measurement and Test Methods	System that enables the efficient conduct of R&D and control of production	*Advanced Combinatorial Testing System (ACTS)*: A NIST system that utilizes combinatorial testing to implement the interaction rule, which holds that most failures are triggered by one or two parameters, and progressively fewer by three or more parameters. The method developed by NIST is used by many organizations to identify software errors.
Standards	Framework of guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization	*Payment Card Industry Data Security Standard*: A worldwide information security standard, defined by the Payment Card Industry Security Standards Council, to "provide an actionable framework for developing a robust payment card data security process—including prevention, detection, and appropriate reaction to security incidents" (PCI-SSC, 2011). NIST maintains a list of Federal Information Processing Standards (FIPS) that it mandates for use in information systems and organizations within the federal government (NIST, 2009b).
Protocols	The set of procedures to be followed when communicating	*Internet Protocol version 6 (IPv6)*: The Internet Protocol (IP) enables data and other information traffic to traverse the Internet and arrive at the desired destination. The current generation of IP, version 4 (IPv4), has been in use for more than 20 years, but the Internet's transformation during this time from a research network to a commercialized network caused some stakeholders to raise concerns about the ability of IPv4 to accommodate emerging demand and security. IPv6 has been selected as a way of meeting these challenges (Deering and Hinden, 1995).
Best Practice Documents	Documents describing techniques, methods, or processes that are commonly agreed upon to improve an organization's cyber security	*Information Security Forum, Standard of Good Practice for Information Security*: Every 2 to 3 years, the Information Security Forum (ISF) (an international, nonprofit organization that supplies authoritative opinion and guidance on all aspects of information security) publishes the Standard of Good Practice for Information Security. This is a detailed documentation of best practices in information security-based research conducted by the ISF benchmarking program (ISF, 2007).
Information Sharing Systems	Organizations and tools that enable the dissemination of information on cyber security threats	*Financial Services Information Sharing and Analysis Center (FS-ISAC)*: The FS-ISAC specializes in disseminating physical and cyber threat alerts and enabling anonymous information-sharing capability across the entire financial services industry (FS-ISAC, 2011).

The focus of this study is on the economic consequences of gaps in the CSTI and the potential benefits of narrowing these gaps. We define a CSTI "gap" as the difference between the current state of a specific CSTI component and an enhanced state, both from security and benefit-cost perspectives. Stated differently, a CSTI gap is the difference between what is now and what would be attainable, given reasonable advances in CSTI R&D productivity.

ES.2 Market Failures Underlying CSTI Inadequacies: The Economic Rationale for Targeted Public and Public-Private Action

While the CSTI clearly has a critical economic role, it has a number of characteristics that discourage private investment in such technical infrastructure, despite its value to society. By its very nature, CSTI is nonexcludable and nonrival: noninvesting 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 value they generate. CSTI creates spillover benefits enjoyed by all firms, but also creates an incentive for firms to "free ride"—to wait for other firms to incur the cost of developing them. Such behavior prolongs the early part of a technology's life cycle and delays the introduction of new products and services. Thus, the profit motive will not provide sufficient incentive to produce CSTI. This market failure relates directly to NIST's mission of developing and fostering critical and equitable technical infrastructure.

NIST's assigned role is to develop infratechnologies and technology platforms that will help U.S. organizations thrive, primarily by reducing bottlenecks that result from barriers to investment. Developing the technical infrastructure that can measure, test, and ensure the quality of products between tiers of a supply chain (e.g., software providers and customer organizations) is essential. Products 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 barriers inhibit the development of sufficient CSTI. For example, coordination problems among providers/users of CSTI prevent the development of novel technology platforms 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 basic and generic platform technologies and also standards to ensure that the threat data needed are both efficiently developed and standardized across software platforms. The private sector is unlikely to invest sufficiently in these areas of CSTI.

CSTI developed by NIST and other organizations enables other public agencies such as DOD and DHS to achieve their national security missions related to cyber security and private firms to make more efficient cyber security investments. Thus, increased public or public-private provision of CSTI will increase the marginal productivity of all private expenditure on cyber security. And, in the aggregate, each dollar devoted to producing a safe cyber environment will result in an even greater increase in the level of cyber security attained.

ES.3 Study Methodology

A four-phase process was adopted for quantifying the economic impact of improving the CSTI. The first phase involved estimating current spending on the CSTI by the public and private sectors. The second phase involved conducting a series of in-depth interviews with cyber security directors in six key industries to identify CSTI gaps and to help develop a national survey instrument. Nine key CSTI gaps were identified as the most important for near-term, targeted investment in infratechnology and technology platform solutions. Insights acquired during this phase guided the development of the analytical focus on a hypothetical 10% improvement in cyber security (as measured by a reduction in incidents and breaches) as the best strategy for collecting economic impact data from companies. In the third phase, we conducted targeted interviews with security experts and organizations to identify specific CSTI improvements that would deliver the improvements. Finally, a broad-based online national survey of IT managers was used to quantify impacts.

Our analysis was bounded by several factors and is therefore not meant to be a comprehensive estimate of the total cost of current cyber security gaps to the United States. First, the study focuses on identifying key gaps that exist in the CSTI, not all cyber security gaps. Second, the gaps were identified by focusing on IT security departments in six industries most likely to be affected by cyber security gaps based on a variety of characteristics, including IT intensity and cyber security spending. Hence, it may not capture all issues for all organizations. Basic research was not addressed. Applied research that improves the efficiency and/or effectiveness of cyber security investments made by all organizations was the focus. The following is a summary of the findings.

ES.4 Annual Public- and Private-Sector Investment in CSTI

In 2012, the federal government, cyber security industry consortia and nonprofits, and private firms invested an estimated $716.1 million in CSTI-related R&D activities (see Table ES-2). The federal government was the largest investor at 70.79% of total CSTI funding ($506.9 million)[5], followed by private firms at 19.93% ($142.7 million), and industry consortia at 9.29% ($66.5 million).

The federal government supports CSTI to ensure that the United States and its citizens can fully use the information technology revolution (White House, 2009). Five federal agencies

[5] The federal portion was obtained from FY2012 budget requests. This approach was taken because budget requests, although not as accurate as authorizations, have more detail, thereby allowing identification of CSTI-related elements.

Table ES-2. Estimated Public and Private U.S. CSTI Spending (2012)

Type of Organization	Estimated CSTI Spending ($ million)	Percentage of Total Spending
Federal government	506.9	70.8
Nonprofit industry consortia	66.5	9.3
For-profit corporations	142.7	19.9
Total	**716.1**	

have major programs that fund research, development, testing, evaluation, and coordination of technical infrastructure activities for broader use by the public and private sectors: the Department of Defense (DoD), the Department of Homeland Security (DHS), National Science Foundation (NSF), Department of Energy (DOE), and the National Institute of Standards and Technology (NIST) (Table ES-3).

Private-sector organizations invest in the CSTI by virtue of their embodiment in proprietary technologies developed for internal use, and private-sector organizations directly support industry-wide CSTI projects and their adoption through funding provided to and participation in industry associations. Labor investments made by the private sector to participate in industry associations and consortia were estimated to be approximately $140 million. Private funding of industry-wide projects and contributions to consortia were not estimated to avoid double counting when reviewing industry association expenditures.

Industry associations and other nonprofit organizations play a smaller role in the CSTI, as measured by expenditures, yet their involvement both directly benefits their industries and indirectly enables public-private coordination. These organizations exist to bring professionals together to carry out technology or policy research, provide precompetitive services, offer education, coordinate activities, and convene discussions. The purpose of these activities is to serve many firms—or entire industries—through aggregated human capital and collective insight. For example, organizations may share threat data with other organizations within an industry, as is the case with Information Sharing and Analysis Centers (ISACs).[6] Industry associations and nonprofit organizations may also engage in policy research; for example, the Internet Society organizes discussions, debates, and papers on Internet security, among other Internet issues.

[6] ISACs were created in 1998 in response to Presidential Decision Directive-63 (PDD-63), signed May 22, 1998. In PDD-63, U.S. critical infrastructure sectors were each asked to establish information sharing organizations to enable the sharing of threat information (physical and cyber) among relevant organizations. See http://www.isaccouncil.org/index.php?option=com_docman&task=doc_download&gid=1&Itemid=.

Table ES-3. Estimated Federal CSTI Spending (2012)

Agency	Spending ($ million)		CSTI Percentage of Total Budget
	Total	Estimated CSTI	
Department of Defense (DoD)*	553,000	212.5	0.038
Defense Advanced Research Projects Agency (DARPA)	3,000	77.7	2.589
Office of the Secretary of Defense (OSD)**	4,649	115.7	2.489
Army	144,900	11.8	0.008
Air Force	149,000	7.4	0.005
Navy	161,400	—	—
Department of Homeland Security (DHS)	57,000	170.0	0.298
Department of Energy (DOE)	29,500	30.0	0.102
National Science Foundation (NSF)	7,800	16.0	0.205
National Institute of Standards (NIST)	1,000	78.3	7.834
Total	**648,300**	**506.9**	**0.078**

Note: Sums may not add to totals due to independent rounding. * Although DoD includes DARPA, OSD, Army, Air Force, and Navy spending, these five subgroups do not add up to the DoD as additional spending was attributed to the DoD itself. **OSD total budget is the sum of procurement, Research, Development, Test & Evaluation (RDT&E), and operations and maintenance funding.

Sources: NIST (2011a), NSF (2011), DOE (2012), DHS (2011a), OSD (2012), DARPA MJ (2011).

ES.5 Industry's and Cyber Security Experts' Recommendations of CSTI Gaps in Critical Need of Targeted Solutions

To help prioritize future public investments in the CSTI, corporate cyber security directors and independent security experts identified CSTI areas that would have significant beneficial impacts on U.S. industry's level of cyber security if the levels of investment were increased. The nine areas are as follows:

- Authentication of all system users
- Sharing of or access to threat data
- Specification and collection of security metrics
- Mobile device security
- Cloud security
- Automated threat detection and prevention
- Protection and mitigation from loss of equipment and media
- Education about IT security best practices and threat awareness

- Standards for meeting auditing and compliance requirements

The existence of investment gaps identified in this study represents CSTI shortfalls that, if left at their current level/size, 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. Table ES-4 presents potential CSTI technologies that, if developed, could narrow the security gap in each of the nine areas by at least 10%.

Prospective economic impacts accruing to the cyber security operations of U.S firms are estimated to be approximately $6.0 billion.[7] As shown in Table ES-5, the largest 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).[8]

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.[9] 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%.[10] A typical company was willing to spend approximately about $1 million to reduce incidents and breaches by 10%.

ES.7 Conclusions and Recommendations

Just improving the effectiveness of the CSTI by 10% would be worth $6 billion to cyber security directors at U.S. firms. This is more than 8 times the $716 million spent on CSTI each

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

[8] Note that 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.

[9] Respondents to the survey fielded between November 2011 and February 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.

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

year by all U.S. parties, suggesting that the social return on successful targeted CSTI investments would be high.

Table ES-4. Recommended CSTI Improvements by Gap Area

Gap Areas	CSTI Improvements Aimed at Addressing Gaps
Cloud security	• Standard for the specification of and/or certifying a cloud provider's security policy and security offerings • Risk-assessment framework for cloud providers • Model of liability agreed upon by the cloud provider
Mobile device security	• Standard specifications for anti-virus protection for mobile devices • Controls on minimum security capabilities for mobile devices/portable media • Usable mobile authentication standards
Specification and collection of security metrics	• Standards to describe metrics in a vendor-independent format • Improved methodology for risk-management-based cyber security
Standards for meeting auditing and compliance requirements	• Standard to map multiple auditing or compliance checklists into one centralized "matrix"
Automated threat detection and prevention	• Recommendations for intrusion detection deployment and operation • Framework for a crowd-sourced or outsourced incident investigation • Tools for helping with the processing of alerts • Standard metrics for intrusion detection and benchmarking
Sharing of or access to threat data	• Standards and protocols for the format of data being shared • Establishment of a trusted broker that can handle collection and dissemination of data • Standard legal agreement for making data anonymous and sharing data
Education about IT security best practices and threat awareness	• Best practices recommendations tailored to specific companies • A high-quality security training standard for end users and management in order to reduce susceptibility to attacks like phishing and social engineering
Authentication of all system users	• Standards for single sign-on • Standards for multi-factor authentication, including combinations of strong passwords, hardware tokens, and biometrics • Policies to support better data sharing among companies and thus enable risk-based authentication through context awareness
Protection and mitigation from loss of equipment and media	• Standards for improved mobile device tracking/wiping capabilities • Standard procedures to support centralized and remote administration of data that is stored or accessed from distributed devices

Table ES-5. Estimated Benefits from a 10% Improvement in CSTI, Extrapolated to Total U.S. ($ million)

Gap Areas	Finance and Insurance	Manufacturing	Retail Trade	Health Care and Social Assistance	Information	Utilities	Total (Key Industries)	Total (All Industries)
Cloud security	256	185	84	82	80	22	709	1,146
Mobile device security	208	150	68	66	65	18	575	928
Specification and collection of security metrics	150	108	49	48	47	13	414	668
Standards for meeting auditing and compliance requirements	147	106	48	47	46	13	407	658
Automated threat detection and prevention	142	102	47	45	44	12	392	633
Sharing of or access to threat data	141	102	46	45	44	12	390	631
Education about IT security best practices and threat awareness	131	94	43	42	41	11	362	585
Authentication of all system users	126	91	41	40	39	11	348	562
Protection and mitigation from loss of equipment and media	42	30	14	13	13	4	117	189
Total	**1,342**	**967**	**441**	**429**	**418**	**117**	**3,715**	**6,000**

Note: Sums may not add to totals due to independent rounding.

Cloud security ($1.1 billion) and mobile security ($928 million) represent areas of significant need as represented by the magnitude of estimated economic benefits in these two CSTI gap areas. Although the benefits estimated are large, perhaps the potential economic impact of improving mobile and cloud security would actually be much greater. Survey data collected from industry suggests that improvements in cloud and mobile security would increase organizations' use of cloud storage and applications by at least 30% and increase organizations' use of mobile technologies by 30%.

As the number, complexity, and potential impact of cyber threats continue to increase, increased public sector involvement and public-private partnerships is essential. Given the public-goods nature of the CSTI, the private sector is likely to underinvest in the CSTI from a social perspective. Individual firms' production of security depends on the total amount of the CSTI in society. Past studies of the role of technical infrastructure suggest that the public sector has higher productivity in producing the CSTI than individual companies do. Public institutions such as NIST have core expertise in developing technical infrastructure components, as compared to private firms, whose expertise is focused on their business model. Thus, public or public-private provision of the CSTI is recommended.

1. INTRODUCTION

U.S. industries spend billions of dollars a year securing their information technology (IT) assets, yet they still suffer significant losses from cyber attacks. The magnitude of these losses is unknown,[11] but the news media are replete with stories about adverse impacts from such attacks, changes in public perception of organizations that are attacked, and the legal and regulatory consequences. According to General Keith Alexander, Chief of the U.S. Cyber Command and Director of the National Security Agency, the United States saw a 17-fold increase in attacks from 2009 to 2011.[12]

Cyber attacks can be targeted at a wide spectrum of organizations critical to the U.S. economy. For example, in September 2012, six large U.S. banks were hit by a series of targeted denial of service attacks that prevented customers from accessing their accounts online.[13] Retailers repeatedly have been targeted by cyber thieves and have suffered the loss of payment information for millions of customers. In 2009, the Operation Aurora attacks[14] targeted dozens of large companies, including Google, Morgan Stanley, Northrop Grumman, and Symantec, seeking to disrupt their operations. Moreover, the possibility of a catastrophic attack is real. The Stuxnet attack[15] on Iranian nuclear facilities in 2010 and the Night Dragon attack[16] that infiltrated five large U.S. energy companies in 2009 demonstrate that unexpected cyber attacks on cyber-physical infrastructure can be successfully launched.

Organizations are vulnerable to attack through externally facing information architectures; attackers identify and hammer upon weaknesses in these architectures to disrupt services or silently gain access to internal networks. Attacks may mimic authorized transactions to steal or destroy information, or they may seek to corrupt software embedded in industrial controllers for buildings, power plants, and manufacturing facilities. Threats also originate from internal sources. Poor network access control policy designs may allow preventable attacks—whether intentional or not—from internal sources to occur. Although organizations cannot

[11] A variety of studies have sought to estimate the size of losses associated with inadequate cyber security. Florenco and Herley (2011) provide an analysis of the many methodological problems with most of the estimates that exist publically, and the researchers summarized their research in a 2012 *New York Times* article available at http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html,. Anderson et al (2012) identify some useful cost data in past cost studies and conclude that the losses are significant, but they note the extreme difficulty in quantifying losses, particularly indirect losses.

[12] See article by Sanger and Schmitt (2012) at http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html.

[13] See article by Perlroth (2012) at http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html.

[14] See http://www.mcafee.com/us/threat-center/operation-aurora.aspx.

[15] See http://www.symantec.com/connect/blogs/w32stuxnet-dossier.

[16] See http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

completely prevent attacks from outside or from within, they can dissuade and fend off attacks through strong defensive postures.

However, the security apparatus protecting networks may itself be an amalgam of solutions assembled over time by successive security personnel. Thus, not only are potential vulnerabilities inherent in software design; they are also associated with the human element in cyber security architecture implementation, operation, and maintenance.

Given the rapidity with which cyber attack techniques evolve, the typical organization may not have the technical capacity, knowledge, or foresight to identify or adequately address attacks on its own. Few organizations are able to maintain a high level of cyber security while maintaining full productivity and product/service offerings. Trade-offs exist between imposing delays on staff, partners, or customers and providing access and services.

The vulnerabilities that make attacks possible are exacerbated by market failures in two related areas. First, individuals and organizations devote too few resources to cyber security. The public-good nature of cyber security and the network externalities inherent in cyber security products and services mean that no individual IT user bears the full risk and cost of insecure IT resources.[17] Indeed, some organizations "free ride" on the cyber security investments of others.

Second, there are inadequate tools and infrastructure—referred to as the cyber security technical infrastructure (CSTI)—needed to efficiently and effectively produce secure cyber environments. Whereas the market failures in the first area affect the level of cyber security that organizations aim to attain, market failures in the second area decrease the efficiency of all investments in cyber security. They create critical gaps in the technical infrastructure that otherwise should enable organizations to detect external threats, detect vulnerabilities created by the software and hardware products that they purchase, and measure the performance of the cyber security measures that they implement.

1.1 Cyber Security Technical Infrastructure

Although specific cyber security systems and architectures may be particular to one organization, a common base of technology, the CSTI, exists that enables more effective and efficient cyber security research, products, services, and operations. CSTI components include standards, operating protocols, test methods, reference data, performance metrics, analytical tools, and information sharing systems (collectively referred to as "infratechnologies"), as well as novel security concepts and precompetitive prototype systems (called "technology platforms" or "generic technologies").

[17] Cyber security products and services here refer to both products and services that are primarily aimed at providing cyber security (e.g., antimalware, firewalls, etc.) as well as all other products that are connected to the internet and may not be developed with security in mind.

The infratechnologies and technology platforms that make up the CSTI have substantial public-good content[18] and collectively raise the level of national cyber security. They support efficiency in cyber security operations and stimulate innovation and competitiveness in the industries that produce related security products and services. The CSTI increases the willingness of firms to invest in developing new security products and increases customers' willingness to pay for these products. In other words, the CSTI stimulates the deployment and diffusion of new technologies.

If the CSTI raises the collective cyber security level, then it follows that areas of CSTI inadequacies represent weaknesses that lower cyber security. Using an armor metaphor, if cyber security is a shield protecting network assets, security software and hardware systems would be the shield's plates, which are held together by bindings—the CSTI. Irrespective of how strong the plates are, gaps in the bindings allow attacks to go through.

The focus of this study is on the economic consequences of gaps in the CSTI and the potential benefits of narrowing these gaps. We define a CSTI "gap" as the difference between the current state of a specific CSTI component and its ideal state, both from security and benefit-cost perspectives. Stated differently, a CSTI gap is the difference between what is now and what would be attainable, given reasonable advances in CSTI R&D productivity.

This NIST study complements technology and policy reviews prepared by the cyber security community by focusing specifically on CSTI gaps and particularly those gaps that the private-sector deems to impose the greatest economic burden on U.S. industry. It does not focus on cyber security overall, only on CSTI. It offers a first-order approximation of the economic benefits to the private sector of narrowing those gaps.

1.2 Previous Policy Reviews and Technical Assessments of Cyber Security Infrastructure Gaps

To date, U.S. government and private-sector technology reviews have focused on cyber security as a whole, identifying challenges and issues based on technical complexity and needs with the aim of offering policy and R&D directions. Notable studies include:

- The Center for Strategic and International Studies' (CSIS's) report *Securing Cyberspace for the 44th Presidency* (2008) provided a high-level assessment of how federal agencies should work together to improve cyber security and offered policy and regulatory recommendations. In a follow-up report, *Cybersecurity Two Years Later* (2010), CSIS highlighted limited progress towards public-private partnerships, information sharing, and self-regulation.

[18] Pure public goods are non-rival and non-excludable; quasi-public goods such as technical infrastructure may be partially rival or partially excludable.

- The White House report, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009), built on the 2008 CSIS report by providing an explicit set of high-level, policy-oriented recommendations for improved coordination of government cyber security activities and increased collaboration between the government and the private sector. This report identified the finance and health care industries, critical infrastructure (e.g., public utilities), and any industry with valuable intellectual property as particularly important.
- The Networking and Information Technology Research and Development (NITRD) Program report, *Cybersecurity Game-change Research & Development Recommendations* (2010), addressed several recommendations from the White House's *Cyberspace Policy Review*. The report identified three prioritized themes for R&D investments: moving target, tailored trustworthy spaces, and cyber economic incentives.
- The Department of Commerce (DOC) report *Cybersecurity, Innovation, and the Internet Economy* (2011) summarized the implementation response to the DOC's Internet Policy Task Force 2010 Notice of Inquiry, outlining a new strategy for protecting the Internet and information innovation sector (I3S). The strategy also includes incentivizing I3S organizations to adopt nationally recognized standards, educating the public and private sectors about I3S vulnerabilities, and continuing U.S. progress in international collaboration.
- The *White House Fact Sheet: Cybersecurity Legislative Proposal* (2011b) outlines a need for a national standard for breach reporting, voluntary government assistance for organizations reacting to security intrusions, protection for organizations that share threat data, and transparency of the cyber security efforts of critical-infrastructure organizations. The report also recommends the development of new privacy and civil liberties procedures that will work in parallel with cyber security measures to protect the confidentiality of individual data when sharing information and to ensure that such data are monitored, collected, used, retained, and shared for cyber security reasons only.

Two additional reports dig deeper into specific technical areas of need and the manner in which the federal government should contemplate potential cyber security investments. A 2011 report from the White House entitled *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program* outlines four major themes for cyber security research: (1) technology with built-in security and assurance proofs, (2) development of dynamic trust environments, (3) technology solutions that shift and change over time, and (4) cyber security incentives for users and organizations based on scientifically sound metrics.

The Department of Homeland Security (DHS) report *A Roadmap for Cybersecurity Research* (2009) provides the most specific, robust assessment of the unresolved problems that underlie existing gaps in the technical infrastructure for cyber security. Specifically, it identifies 11 difficult problem areas awaiting resolution:

1. *Scalable trustworthy systems*—how can the security of systems be maintained or improved as they become larger and more complicated?
2. *Enterprise-level metrics*—what metrics can be identified to improve management cyber security assessments and investment analyses?
3. *System evaluation life cycle*—how can all IT systems be evaluated in a comprehensive way that includes a clear understanding of security from adoption to retirement?
4. *Combating of insider threats*—how can insider threats be more quickly and easily identified and prevented?
5. *Combating of malware and botnets*—how can detection and mitigation of the effects of malware and botnets become more effective and efficient?
6. *Global-scale identity management*—how can identity management within and across organizations and by the public be made more efficient and effective?
7. *Survivability of time-critical systems*—how can critical systems be designed to allow continuous functionality after a successful attack has occurred?
8. *Situational understanding and attack attribution*—how can the tracking and attribution of attacks be improved?
9. *Provenance*—how can data used in analyzing security threats and solutions be improved to enable clear source information?
10. *Privacy-aware security*—how can privacy be built in to products and services more seamlessly for software producers and users?
11. *Usable security*—how can all security products and services be made to be more usable by individual and organizational users?

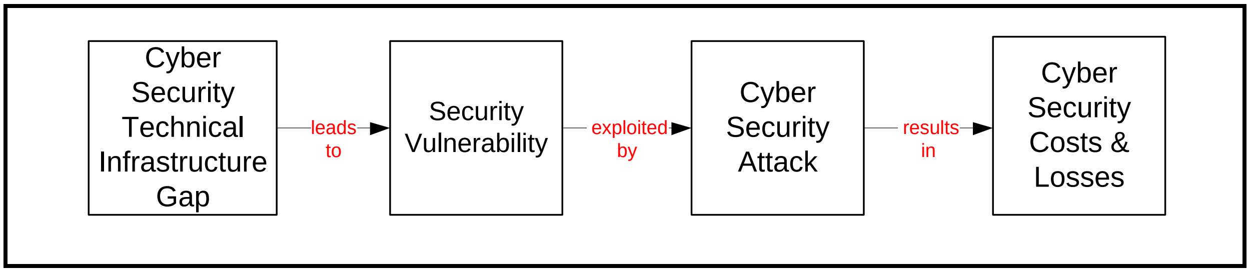
Furthermore, this DHS report identifies future security problems associated with emerging computing platforms, such as virtualization (cloud computing), mobile devices, and social networking.

These important assessments address critical issues in cyber security and to some degree also address CSTI. But, beyond qualitative discussions or implied references to the economic significance of the technical issues, none reviewed the economic consequences of gaps, let alone quantified them.

1.3 An Economic Approach to Identifying and Quantifying the Consequences of CSTI Gaps

We developed a framework that conceptualizes the connection between CSTI gaps and potential improvements that, if addressed, would benefit industry by improving the level of cyber security. Attacks seek to exploit vulnerabilities, such as insufficient end-user security and inadequate software quality. Figure 1-1 depicts how gaps in the CSTI result in cyber security

Figure 1-1. Connecting CSTI Gaps to Economic Costs and Losses: A Conceptual Framework



Cyber Security Technical Infrastructure Gap: The difference between the current state or level of the CSTI and the ideal state or level, from a security perspective (e.g., insufficient security to minimize security vulnerability).

Vulnerability: A security weakness (e.g., inadequate software quality, end-user insecurity).

Cyber Security Attack: Exploitation of a vulnerability (e.g., virus, denial-of-service attack).

Cyber Security Costs and Losses: Economic damage caused by an executed threat (e.g., theft of personal information, disruption of service or functionality).

costs and losses. An organization is affected by gaps in the CSTI when it incurs excessive costs to avoid attacks or to react to an attack (e.g., a virus) that is initiated by someone wishing to cause harm (e.g., disrupt a network or service) or illegally access or obtain information (e.g., documents or e-mails). These attacks seek to exploit vulnerabilities, such as insufficient end-user security and inadequate software quality. Narrowing gaps in the CSTI will result in economic benefits.

Spending on cyber security as a percentage of total IT spending has remained steady for several years—currently approximately 5.2% of company IT spending according to Gartner. On a per-employee basis, organizations worldwide spent approximately $591 per employee on cyber security in 2011, including labor, capital, and services (Guevara, Hall, & Stegman, 2012).

When an attack is successful, the losses can be large. A 2005 Department of Justice (DOJ) Bureau of Justice Statistics (2008) survey of more than 3,000 businesses estimated that the businesses had experienced a median loss of $6,000 and 16 hours of downtime from cyber attacks.

Given the magnitude of the realized and potential aggregated costs and losses associated with cyber threats and attacks, this study attempts to offer a new perspective on prioritizing public investments in the CSTI by analyzing the economic impact of existing CSTI gaps and estimating the benefits of narrowing these gaps.

1.4 Study Objectives, Scope, and Limitations

This study had three primary objectives that supported the goal of characterizing the economic consequences of an inadequate CSTI:

- estimate current expenditures on CSTI R&D and coordination activities by the federal government, industry consortia, and the private sector;
- identify CSTI gaps that the private sector expects to impose the greatest economic burdens on U.S. industry; and
- estimate the economic benefits of narrowing those gaps.

Between January and October 2011, the RTI study team of economists and cyber security researchers engaged private-sector cyber security directors and academic researchers in semistructured interviews to review CSTI issues. These interviews identified CST gaps and supported the development of a survey that IT security managers would be able to respond to more broadly. The survey posed questions to security managers about how much their organizations would benefit from a 10% improvement in cyber security, as measured by a reduction in the number of IT security incidents. The survey results were paired with expert interview findings about CSTI improvements that could deliver that improvement. Ultimately, this study provides an economic perspective on CSTI inadequacies that complements the technical and policy reports referenced in the previous discussion.

Our analysis was bounded by several factors and is therefore not meant to be a comprehensive estimate of the total cost of current cyber security gaps to the United States. First, the study focuses on identifying key gaps that exist in the CSTI, not all cyber security gaps. Second, the gaps were identified by focusing on IT security departments in six industries most likely to be affected by cyber security gaps based on a variety of characteristics, including IT intensity and cyber security spending. Hence, it may not capture all issues for all organizations. Basic research was not addressed. Applied research that improves the efficiency and/or effectiveness of cyber security investments made by all organizations was the focus.

1.5 Report Organization

The report is divided into eight major sections:

- Section 2 defines and characterizes the CSTI and provides an economic framework for investments in the CSTI.
- Section 3 describes the study methodology.
- Section 4 provides a conceptual discussion of the rationale for government support of the CSTI.
- Section 5 lists and summarizes current spending on the CSTI.
- Section 6 characterizes the nine gaps in the CSTI identified in this study and describes potential CSTI solutions to help fill the gaps.
- Section 7 summarizes the results of our analysis of the economic benefits of narrowing the current gaps in the CSTI.
- Section 8 provides concluding remarks and policy recommendations.

2. CHARACTERIZING THE CYBER SECURITY TECHNICAL INFRASTRUCTURE

The CSTI is an example of what is sometimes called an “industrial commons”[19]: the embedded knowledge and technology framework that enhances the efficiency, effectiveness, and productivity of the proprietary capital and labor that use it. The CSTI supports an organization’s ability to detect threats, and provides some level of assurance that its systems adhere to best practice. For example, the CSTI supports the communication of threats by establishing a protocol that network operators follow to assess, measure, and communicate those threats. The CSTI does not include the central server operations of any one firm, nor does it include the workforce assigned to monitor, detect, and investigate intrusions. It is a common set of technologies, standards, policies, and procedures that competing firms draw upon to achieve a more secure environment for their organizations, partners, and customers. The distinction between the CSTI and physical assets is important because in common IT-industry parlance, technical infrastructure refers to physical assets such as servers, desktops, cabling, and software systems.

2.1 Overview of Cyber Security and Cyber Security Threats

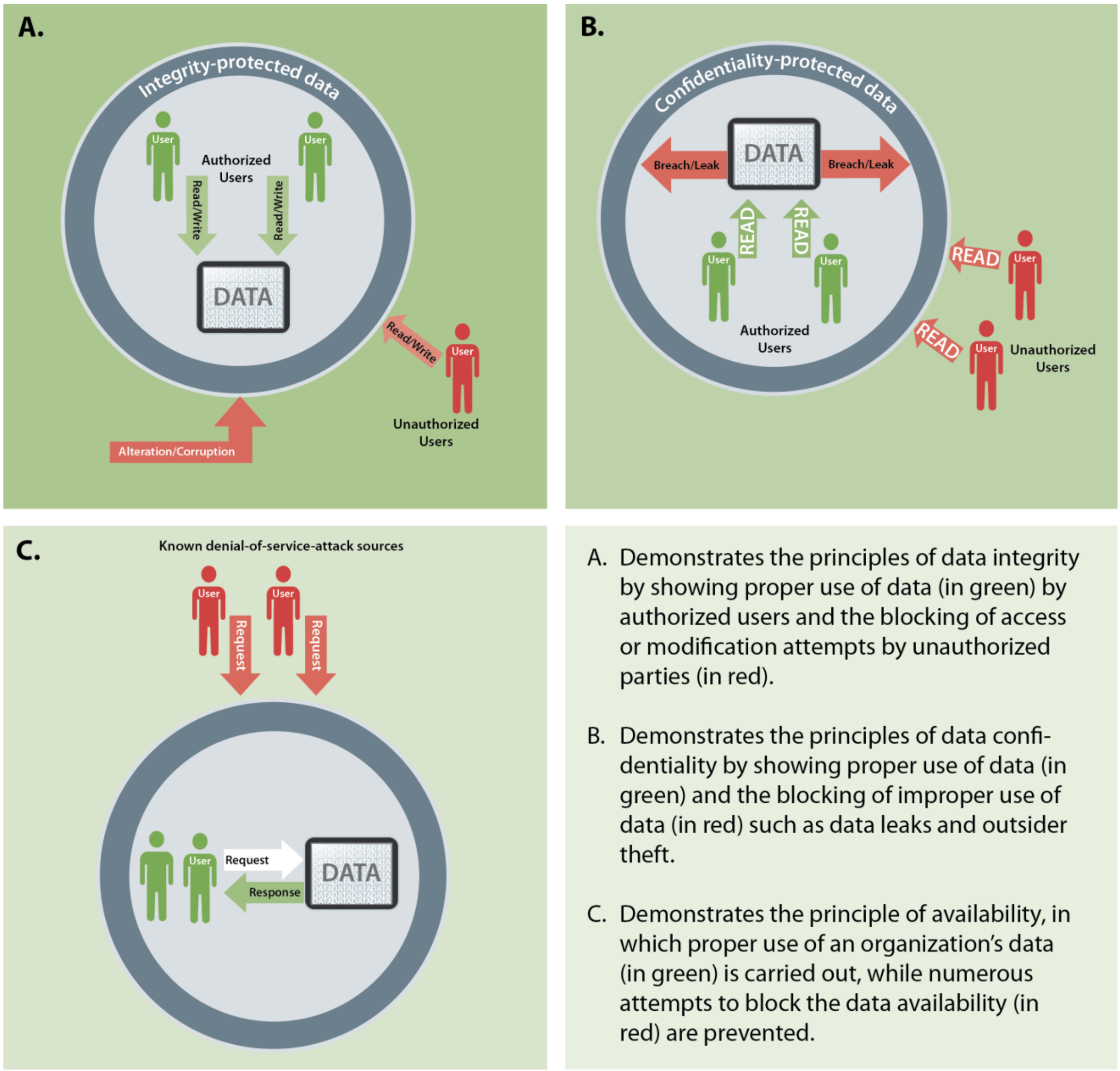
Although the focus of this report is on CSTI, some familiarity with cyber security is necessary to understand the implications of CSTI inadequacies. Cyber security (also called “IT security” or “information security”[20]) refers to the process of securing electronic resources from unauthorized access, modification, or destruction. These resources include the hardware and software necessary to store, transfer, and manipulate data. The U.S. Code defines information security as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction” in order to provide

- “*integrity*, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- *confidentiality*, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- *availability*, which means ensuring timely and reliable access to and use of information” (Office of the Law Revision Counsel, 2011) (Figure 2-1).

[19] See Pisano and Shih (2009).

[20] The term “information security” can be used to encompass cyber security as well as the security of assets not attached to a network (e.g., important paper documents), though most important information assets are saved on network resources today.

Figure 2-1. Cyber Security: Maintaining Data Integrity, Confidentiality, and Availability



A. Demonstrates the principles of data integrity by showing proper use of data (in green) by authorized users and the blocking of access or modification attempts by unauthorized parties (in red).

B. Demonstrates the principles of data confidentiality by showing proper use of data (in green) and the blocking of improper use of data (in red) such as data leaks and outsider theft.

C. Demonstrates the principle of availability, in which proper use of an organization’s data (in green) is carried out, while numerous attempts to block the data availability (in red) are prevented.

Source: RTI International.

Cyber security threats, attacks, and incidents may be categorized as *insider* or *outsider*. The Internet Engineering Task Force (IETF) (2000) defines an insider attack as one which is initiated “by an entity inside the security perimeter.” These entities can be employees, vendors, or contractors whose positions give them access to an organization’s resources, whether or not that access was authorized. Incidents from insider threats may be accidental or malevolent. For example, organizations may lose data because employees lose devices that store sensitive data.

Outsider threats are risks of attacks and incidents originating from users accessing an organization’s data and resources from outside the organization. The IETF (2000) defines an outsider attack as initiated “from outside the perimeter, by an unauthorized or illegitimate user of the system." In an interconnected world, many resources are connected to the worldwide web to enable a more productive exchange of information among employees, partners, and customers. These attacks often exploit vulnerabilities in an area of the organization's network that is connected to the Internet.

There are various ways to carry out an attack on an organization's IT resources and data. A 2010 survey conducted by *CSO Magazine* in collaboration with the U.S. Secret Service, US-CERT, and Deloitte explored firms' perceptions of the types and sources of cyber attacks. The survey, the results of which are presented in Table 2-1, compiled a listing of attacks and their sources as described by 523 respondents worldwide.[21] Respondents were asked if they experienced any of the cyber crimes listed and, if so, these were asked about their perception of the origins of those crimes. The most frequent attacks come from viruses, worms, and other malicious code, followed by spyware, phishing, and inside attacks, such as unauthorized access to or use of information, systems, or networks and unintentional exposure of private or sensitive information. Of note, the 2010 CSO survey found that a significant number of organizations did not think that they had been attacked by certain types of threats or were unsure if they had been attacked.

Viruses and worms are particularly concerning. A virus is defined as a "self-replicating code segment that causes a copy of itself to be inserted in one or more other programs" (Vogel, 2010). A virus can be, but is not always, malicious. A worm is defined as "a program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability, or availability" (Vogel, 2010). Unlike a virus, a worm does not need to replicate itself, but rather is a self-contained program capable of causing damage. A virus or worm can be used to steal, manipulate, or destroy information, or it can take control of or destroy systems.

Denial-of-service (DoS) attacks are used to overload servers with illegitimate data requests, preventing them from processing legitimate user requests. DoS attacks generally involve one or more botnets—a group of computers hijacked by a hacker used to launch additional attacks, send spam, or pursue other malicious purposes. Some botnets have used 100,000 or more compromised host computers (bots) to engage in DoS attacks or spread malware.[22] Although most botnets are composed of home computers, many business computers are suspected of being active bots.

[21] More recent data in this format was not available at the time this report was published.

[22] Constantin (2011) describes a botnet taken down in September 2011 that included 110,000 compromised hosts. And Messmer (2009) lists several botnets estimated to include up to 3.6 million compromised hosts at the time of the article.

Table 2-1. Percentage of Companies Having Experienced Common Types of Threats/ Attacks and Threats'/Attacks' Perceived Sources

Cyber Security Threats and Attacks	Experienced this Threat or Attack (%)	Source of Attack, %				
		Insider	Outsider	Source Unknown	N/A	Don't Know
Viruses, worms, or other malicious code	53	15	41	19	13	15
Spyware (not including adware)	41	15	28	13	23	23
Phishing (someone posing as a person's company online in an attempt to gain personal data from that person's customers or employees)	38	5	33	11	31	21
Unauthorized access to/use of information, systems, or networks	35	23	13	6	36	23
Unintentional exposure of private or sensitive information	34	29	3	5	40	22
Illegal generation of spam e-mail	32	7	26	9	37	21
Denial-of-service attacks	27	5	23	11	41	21
Financial fraud (e.g., credit card fraud)	26	11	16	4	46	24
Theft of intellectual property	22	16	6	4	48	26
Zombie machines on organization's network/ bots/use of network by botnets	22	7	17	8	47	23
Theft of other (proprietary) information, including, for example, customer records and financial data	21	15	5	4	51	25
Theft of personally identifiable information (PII)	20	10	11	4	51	26
Sabotage: deliberate disruption, deletion, or destruction of information, systems, or networks	19	10	10	5	55	21
Intentional exposure of private or sensitive information	16	11	6	4	56	23
Website defacement	14	2	12	3	61	22
Extortion	5	1	3	1	71	23
Other	4	2	2	2	56	39

Source: *CSO Magazine*. 2010. 2010 Cyber Security Watch Survey—Survey Results. Available at http://www.csoonline.com/documents/pdfs/2010CyberSecurityResults.pdf.

In response to the pervasiveness and multifarious character of cyber security threats, companies employ a variety of automated and manual methods to protect their information and resources. All of these methods are based on or use products or services supported by the CSTI. Defining what we mean by the "cyber security technical infrastructure" is imperative to establishing the scope of this study.

2.2 Components of the Cyber Security Technical Infrastructure

Technical infrastructure is generally defined as the elements of an industry's technology base that are jointly used by competing firms. The CSTI spans many industries; specific CTSI infrastructure components are often used by heterogeneous organizations. Tassey (2007, 2008) identifies three major elements of technical infrastructure:

- **Technology platforms**, sometimes referred to as generic technologies, represent the first phase in a technology's development, usually taking the form of a laboratory proof of concept that is derived from basic science.
- **Infratechnologies** are a varied set of "technical tools" that enable the development and efficient use of technology at all stages of economic activity. Examples include measurement and test methods, and scientific and engineering databases that underlie the development and implementation of industry standards.
- **Proprietary technologies** consist of methods, processes, and techniques firms develop to achieve their strategic objectives in conducting the development and production processes. Competing firms differentiate themselves through their implementation of these proprietary technologies.

At times, the distinctions between these three technology elements can be blurred. Commercial products and services are derived from an underlying technology platform and are supported by a range of infratechnologies. These latter two elements typically exhibit some combination of proprietary and public-good technology content. This quasi-public technology character often obscures the boundaries between public and purely proprietary technology elements (Tassey, 2007, 2008). The discussion that follows explores technology platforms and infratechnologies in greater depth.

2.2.1 Technology Platforms

As described above, a technology platform represents the culmination of early-phase R&D that results in a proof-of-concept. Technology platforms are high-level, functional prototypes that demonstrate new applications but usually do not have a well-defined market application. They are precommercial, meaning that they have yet to be sufficiently adapted and engineered for one market or one specific application. Functional prototypes being offered to multiple users for review and evaluation are a good example of a generic or platform technology. Ultimately, these platforms become sufficiently developed so that proprietary technologies can be developed.

A technology platform is nonrival and is considered only partially excludable (that is, it may be accessible by those who do not pay for it); thus, it is considered a quasi-public good. This partial excludability is beneficial; because the technology is somewhat freely available, it encourages multiple avenues of innovation. However, this complicates the financing of technology platform development because industry emphasizes the funding of private or excludable goods with sufficient intellectual property protections.

Role-Based Access Control (RBAC) is an example of a technology platform that is part of the CSTI. Prior to RBAC, many companies manually set and adjusted individual employees' access to certain IT resources. RBAC proposed that organizations establish standard levels of access (permissions) to the various computing resources and networks of an organization that are tailored to specific employee roles or job functions rather than to each specific individual. In a large, information-intensive organization, it is generally far easier and more reliable for system security managers to assign a new hire to one or more “roles” and have all the appropriate permissions set automatically than to do each manually. The RBAC framework (the technology platform), supported by NIST, allowed these increases in efficiency and effectiveness, through specific commercial implementations, to be achieved.[23]

Technology platforms are used both in developing infratechnologies and in developing new market applications. Therefore, technology platform gaps or deficiencies often result in impeding the creation of new cyber security products as well as new infratechnologies.

2.2.2 Infratechnologies

Infratechnologies are a set of technology elements that composes an industry’s technical infrastructure, or technology that supports industry processes from R&D to manufacturing and commercialization. In the cyber security arena, the five broad categories of infratechnologies are (1) measurement and test methods, (2) standards, (3) protocols, (4) best practice documents, and (5) information-sharing systems. See Table 2-2 for examples of CSTI in each of these infratechnology categories.

Infratechnologies result from investments by numerous private, public, and governmental organizations. Standardization activities are an excellent example. In some cases, standards are enforced by the government. Cyber security for federal government agencies is enforced by the Office of Management and Budget and by self-reporting to independent regulatory organizations (e.g., electric utilities’ cyber security compliance is reported to the North American Electric Reliability Corporation, or NERC). In the federal government, NIST maintains a list of standards entitled Federal Information Processing Standards (FIPS) that are “compulsory and binding for federal agencies” (NIST, 2009); NIST also publishes special publications that act as guides for implementing standards, which are compulsory if mandated by a FIPS.

Credit card payment standards are an example of private-sector led standardization activities. In the payment card industry (PCI), the Payment Card Industry Data Security Standard (PCI DSS) was created by the Payment Card Industry Security Standards Council to help PCI organizations prevent credit card fraud. With public- and private-sector support, including that from NIST, PCI standards were developed to provide a shared IT security infrastructure component. Although adoption of PCI standards was voluntary, market forces drove widespread

[23] See more information on RBAC in a 2011 economic impact study of RBAC (O’Connor and Loomis); available at http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf.

adoption; today, no retail vendor can accept credit cards without being compliant. Similarly, in the electric utilities sector, the North American Electric Reliability Corporation (NERC)[24] has established cyber security standards for electric utilities in the United States that aim to provide a framework for identifying and protecting "critical cyber assets" to support reliable operation of the bulk electric system (NERC, 2011).

The examples in Table 2-2 also illustrate the economic importance of each of these infrastructural components. Without PCI, credit card companies might have been suspected of being less secure (e.g., more breaches might have occurred); if so, use of credit cards for online transactions might have been significantly lower over the last decade. The fundamental nature of these infrastructural components implies that deficiencies in them could lead to significant economic costs across multiple competing firms.

Table 2-2. Cyber Security Infratechnology Overview

Type	Description	CSTI Examples
Measurement and Test Methods	System that enables the efficient conduct of R&D and control of production	*Advanced Combinatorial Testing System (ACTS)*: A NIST system that utilizes combinatorial testing to implement the interaction rule, which holds that most failures are triggered by one or two parameters, and progressively fewer by three or more parameters. The method developed by NIST is used by many organizations to identify software errors.
Standards	Framework of guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization	*Payment Card Industry Data Security Standard*: A worldwide information security standard, defined by the Payment Card Industry Security Standards Council, to "provide an actionable framework for developing a robust payment card data security process—including prevention, detection, and appropriate reaction to security incidents" (PCI-SSC, 2011). NIST maintains a list of FIPS that it mandates for use in information systems and organizations within the federal government (NIST, 2009b).
Protocols	The set of procedures to be followed when communicating	*Internet Protocol version 6 (IPv6)*: The Internet Protocol (IP) enables data and other information traffic to traverse the Internet and arrive at the desired destination. The current generation of IP, version 4 (IPv4), has been in use for more than 20 years, but the Internet's transformation during this time from a research network to a commercialized network caused some stakeholders to raise concerns about the ability of IPv4 to accommodate emerging demand and security. IPv6 has been selected as a way of meeting these challenges (Deering and Hinden, 1995).

(continued)

[24] See more information on NERC at http://www.nerc.com.

Table 2-2. Cyber Security Infratechnology Overview (continued)

Type	Description	CSTI Examples
Best Practice Documents	Documents describing techniques, methods, or processes that are commonly agreed upon to improve an organization's cyber security	*Information Security Forum, Standard of Good Practice for Information Security*: Every 2 to 3 years, the Information Security Forum (ISF) (an international, nonprofit organization that supplies authoritative opinion and guidance on all aspects of information security) publishes the Standard of Good Practice for Information Security. This is a detailed documentation of best practices in information security-based research conducted by the ISF benchmarking program (ISF, 2007).
Information Sharing Systems	Organizations and tools that enable the dissemination of information on cyber security threats	*Financial Services Information Sharing and Analysis Center (FS-ISAC)*: The FS-ISAC specializes in disseminating physical and cyber threat alerts and enabling anonymous information-sharing capability across the entire financial services industry (FS-ISAC, 2011).

2.3 Study Focus on Technology Platforms and Infratechnologies

Technology platforms and infratechnologies are critical components of the CSTI. As will be explored in the next section, there is reason to believe that both types of technical infrastructure will be underprovided by the private sector because of their quasi-public-good nature. This fact brings about an underinvestment by the private sector and even by industry associations, because the benefits of such investments cannot be fully appropriated by the innovator.

2.4 NIST's Role in CSTI Provision

Historically, NIST has played a key role in the provision of technical infrastructure. NIST's focus as an organization is to develop infratechnologies and technology platforms that will help U.S. organizations thrive, primarily by reducing barriers that result from market failure. In this section, we provide real-world examples that suggest a need for NIST's involvement in improving the level of CSTI.

As described above, CSTI is in many respects a public good and faces clear network externalities. Broadly, as a result, the private sector provides too low a level of CSTI, and therefore cyber security, and creates a rationale for government involvement in improving that security. Currently U.S. government agencies—primarily the Department of Homeland Security and the Department of Defense—are working to improve the level of cyber security through a variety of efforts, including educational initiatives and investments in improving the cyber security of U.S. government agencies (which results in an overall improvement of all cyber security given the public-good nature). Additional government involvement, including regulation—e.g., requiring reporting of incidents and meeting a certain level of security—is being discussed.

A “weak link” in these efforts is often the fact that the CSTI that underlies an organization’s level of cyber security is insufficient. Differentiating broadly between insufficient cyber security and insufficient CSTI can help to identify the role(s) that government can play in improving cyber security through direct investments in cyber security or indirect investments (e.g., in the CSTI).

Looking at a set of specific attacks can clarify the role of the CSTI more easily. Table 3-1 offers an overview of several recent attacks that have resulted from inadequate CSTI. Broadly, a typical cyber attack usually involves three key stakeholders:

1. An organization that has a set of key assets
2. A supplier of software or hardware with embedded software, which the organization purchases
3. The organization’s employees.

Most attacks involve the use of both technical and non-technical techniques (including all of the attacks listed in Table 2-3). Hackers often exploit coding errors and security weaknesses in the software—e.g., office productivity software and Internet software/plug-ins—and hardware with embedded software—e.g., industrial controllers—purchased by organizations to initiate an attack on the organization with the aim of either stealing critical information or causing actual physical damage. After identifying the technical exploit, the hackers might then identify a common but lax employee-security practice to initiate the attack. For example, the technical exploit could be embedded in a file that could be inserted into a company network by an employee connecting an infected device (e.g., a USB drive) to the company network, an employee opening an infected e-mail attachment, or an employee visiting a malicious website.

In the common example above, the critical market failures are information asymmetry and imperfect information, which occur between tiers of the supply chain—software and embedded software providers and their customer organizations. The customer organizations that purchase and use the software and hardware with embedded software have no way of knowing if or how errors in the software code will create critical cyber insecurities. These organizations lack the tools necessary to measure the quality aspects of common software related to cyber security. This is exacerbated when employees at the target organization are manipulated through social engineering to engage in poor security practices.

Many well-known cyber attacks have exploited weaknesses in the common office and Internet software products developed by companies such as Microsoft, Adobe, and Apple. Other software products which are not as well-known have also come under attack. For example, smart manufacturing software has recently come under attack; such software is designed to be open and easily reconfigurable; however, this makes quality and security maintenance more

Table 2-3. Recent Examples of Cyber Attacks, Exploitation, and Impact

Attack	Target	Weakness/Zero Day Exploited	Social Engineering Factor	Impact
RSA (2011)	RSA	Microsoft Excel, Adobe Flash	Employee opened a spear-phishing e-mail[1] and an attached Excel spreadsheet.	Compromised RSA algorithms putting companies using RSA technologies at risk.
Stuxnet (2010)	Non-networked Iranian nuclear facilities	Windows XP and Windows 7, embedded software in industrial controller	Flash drives with Stuxnet were plugged into Iranian nuclear facilities not connected to the Internet.	Compromised industrial controllers were used to destroy Iranian centrifuges by operating them at critical levels while sending “All OK” signals to monitoring systems.
Night Dragon (2010)	U.S. energy companies	Remote administration tools (RATs)	Several techniques were used including spear-phishing emails[1].	Stole corporate documents such as operational oil and gas field production systems and financial documents related to field exploration and bidding.
Aurora (2009)	Google, Adobe Systems, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical	Microsoft Internet Explorer	Employees opened a spear-phishing e-mail[1] and clicked on web links to malicious websites.	Stole e-mails and other corporate intellectual property (e.g., Google source code).
iPhone hack (example attack)	Apple iPhone	Malicious code placed within a PowerPoint presentation that would scan as normal	iPhone users who opened a spear-phishing e-mail[1] with a pdf file attached would be infected.	Allowed hacker to control iPhone and steal contacts and e-mails (done as part of a contest to identify and exploit weaknesses to prevent the malicious exploitation of the weakness).

[1] Spear-phishing e-mail messages are targeted e-mail messages with links or attachments that when clicked on or executed result in malicious software being downloaded or run on the host computer.

difficult. Because organizations purchasing software lack the ability to measure the security attributes of software products (e.g., the number of security vulnerabilities), the incentive to produce error-free software is further weakened.[25]

Developing the technical infrastructure that can measure, test, and assure the quality of products between tiers of a supply chain (customer organizations and software providers) 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. By enabling stakeholders to measure errors in software, ascertain the quality of software regarding cyber security, and fully understand the nature of vulnerabilities, CSTI creates the incentive for software suppliers to compete along this critical dimension of quality and increases the effectiveness and efficiency of all stakeholders' production of secure cyber environments.

Beyond the need for additional tools to measure quality, additional market failures affect the development of sufficient CSTI. For example, a coordination market failure prevents the development of novel technology platforms 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 basic and generic technologies and also standards to ensure that the threat data needed is standardized across software platforms. The private sector is unlikely to invest sufficiently in these areas of CSTI; however, NIST is well suited to these tasks.

[25] See NIST (2002) for additional discussion of the lack of incentives for software producers to sell higher quality software (i.e., free of bugs, including security related bugs). Available at http://www.nist.gov/director/planning/upload/report02-3.pdf.

3. RATIONALE FOR PUBLIC PROVISION OF CYBER SECURITY TECHNICAL INFRASTRUCTURE

This section reviews the economic rationale for public provision of CSTI. By its very nature, CSTI is nonexcludable and nonrival: noninvesting 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 value they generate. CSTI creates spillover benefits enjoyed by all firms, but also creates an incentive for firms to "free ride"—to wait for other firms to incur the cost of developing them. Such behavior stretches out the early part of a technology's life cycle and delays the introduction of new products and services. Increased public provision of CSTI will increase the marginal productivity of all private expenditure on cyber security. And, in the aggregate, each dollar devoted to producing a safe cyber environment will result in an even greater increase in the level of cyber security attained.

3.1 Economic Model of Investments in the CSTI

Building on the definitions of cyber security, cyber threats, and the role of the CSTI, this section provides an economic framework for thinking about the production of cyber security.

To produce cyber security, firms combine purely private inputs—including proprietary technologies and traditional inputs to the production process—that are competitively supplied with other technical infrastructure. We model technical infrastructure as a public good in the classical sense: it is at least partly nonexcludable and nonrival. This model, described below, was constructed to highlight the key features of the CSTI, and as such, it does not incorporate partial rivalry or excludability.

In principle, technical infrastructure can be either publicly or privately provided. Thus, we will initially consider the case of private provision and then consider how this private equilibrium compares with public provision. In the private equilibrium, firms take the actions of other firms as given; that is, they do not consider the impact their own provision of inputs to the production of CSTI has on the supply decisions of other firms.

For simplicity, suppose two firms have the following production functions for cyber security[26]:

$$CS_1 = I^1(a_1, B^{Total}) \tag{3.1}$$

$$CS_2 = I^2(a_2, B^{Total}) \tag{3.2}$$

[26] The conceptual discussion in this section is based on Anderson (2012) and Tassey (2008).

where a_i represents a vector of private inputs and B^{Total} represents the total amount of technical infrastructure available. Because technical infrastructure is a public good, each firm has access to the same aggregate amount. Although we could specify a general functional form for the production of technical infrastructure, $B^{Total} = f(b)$, where b_i is a vector of individual firms' contributions, we can make all of the key points with a very simple functional form for a two-firm industry:

$$B^{Total} = b_1+b_2 \tag{3.3}$$

Note that, in this simple model, the production functions obey all of the classic assumptions for production technology with one natural exception. Each firm's production of cyber security depends on the total amount of CSTI. Thus, our only assumption apart from a standard production model is that CSTI (B^{Total}) is a public good (e.g., nonrival, nonexcludable). In what follows, a_1 and a_2 are vectors of private inputs to the production of cyber security for firms 1 and 2.

The standard maximization problem for the industry is:

$$Max\ I^1(a_1, B^{Total}) + I^2(a_2, B^{Total}) \tag{3.4}$$

subject to

$$TC=P_a(a_1 + a_2) + P_b*B^{Total} \tag{3.5}$$

$$B^{Total} = b_1 + b_2 \tag{3.6}$$

That is, the objective is to maximize cyber security subject to the budget constraint (Equation 3.5) and the total technical infrastructure (Equation 3.6).[27] The first order conditions (FOCs) for the private maximization of security subject to the constraints are (where subscripts denote first derivatives):

$$\text{Firm 1: } I^1_{a1}=P_a\ ;\ I^1_{b1} = P_b \tag{3.7}$$

$$\text{Firm 2: } I^2_{a2}=P_a\ ;\ I^2_{b2} = P_b \tag{3.8}$$

The solution to these indicates that the price ratio is equal to the private marginal rate of technical substitution between the CSTI and private inputs:

[27] Please note that we could have also specified this as a cost minimization problem—that is, minimize (Equation 3.5) subject to (Equation 3.4) and (Equation 3.6). See Gallaher et al. (2008) for a discussion of the implications of maximizing security given a fixed budget versus minimizing cost given a target level of security.

$$P_b/P_a = I^1_{b1}/I^1_{a1} = I^2_{b2}/\, I^2_{a2}. \tag{3.9}$$

The FOCs that maximize societal cyber security are different, as the social planner[28] considers the impact of each firm's provision of the CSTI on the other firm's security production function. That is, the social planner acknowledges that one firm's investment in CSTI increases the productivity of all private investments in cyber security. Therefore, the FOCs are

$$\text{Firm 1: } I^1_{a1} = P_a \,;\, I^1_{b1} + I^2_{b2} = P_b \tag{3.10}$$

$$\text{Firm 2: } I^2_{a2} = P_a \,;\, I^2_{b2} + I^1_{b1} = P_b \tag{3.11}$$

$$P_b/P_a = (I^1_{b1} + I^2_{b2})/I^1_{a1} = (I^1_{b1} + I^2_{b2})/I^2_{a2}. \tag{3.12}$$

3.2 Demonstrating Underprovision of the CSTI

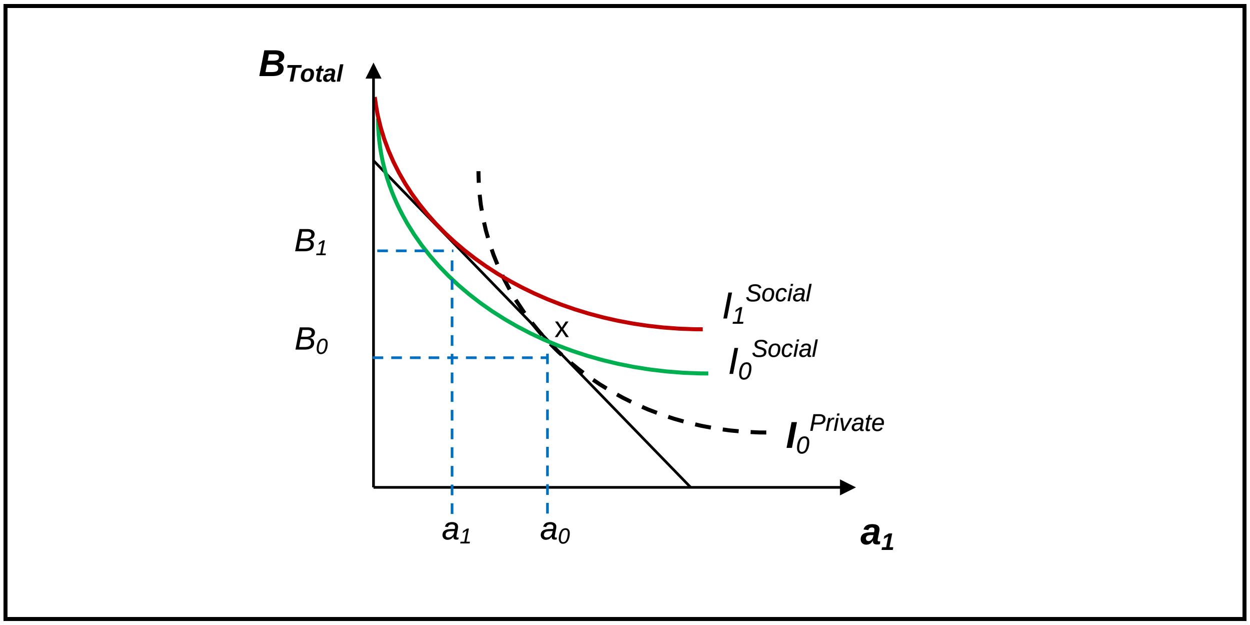
Given the above framework, it is straightforward to show that the level of technical infrastructure that maximizes cyber security from the point of view of society is greater than the amount that would result from the private solution. To see this, consider the iso-security curves that would result from the private and societal maximization problems (in Figure 3-1). For any pair (*a*, *B*), the private marginal rate of technical substitution between cyber security good *a* and CSTI good *B* will be less than the public marginal rate of technical substitution. Along a private iso-security curve, firms are too willing to give up *B* (CSTI) to get more private input to security production *a* because they do not consider the impact the decline in the CSTI has on other firm's ability to produce cyber security.

In this case, at any point, the social iso-security curve (I_0^{Social}) will intersect the private iso-security curve ($I_0^{Private}$) from below (point *X* in Figure 3-1).[29] Therefore, it is possible—with no change in total expenditure—to achieve a higher level of societal security with a lower quantity of private inputs to security production (a_0 *to* a_1) and a higher quantity of the CSTI (B_0 *to* B_1). This occurs at the tangency of the budget line and I_1^{Social}. Alternatively, although point *X* represents a solution to a private firm's cost minimization, this point does not minimize the cost of providing security level I_0^{Social} from the societal point of view. To see this, simply shift the existing budget line inward to a point of tangency with I_0^{Social}.

[28] The "social planner" refers to a fictitious actor making decisions from the perspective of the optimal social good. See discussion in Romer (1987).

[29] To see this, consider the slope of the societal iso-security curve: $dB^{Total}/da_i = I^i a_i/(I^i_{BTotal} + I^j_{BTotal})$. Note that as long *as* $I^j_{BTotal} > 0$, which will be true at an optimum, the slope of the societal iso-security curve will be less than the private iso-security curve. This condition is based on fact that the marginal product of technical infrastructure is positive.

Figure 3-1. Private and Social and Marginal Rates of Substitution of Cyber Security Inputs



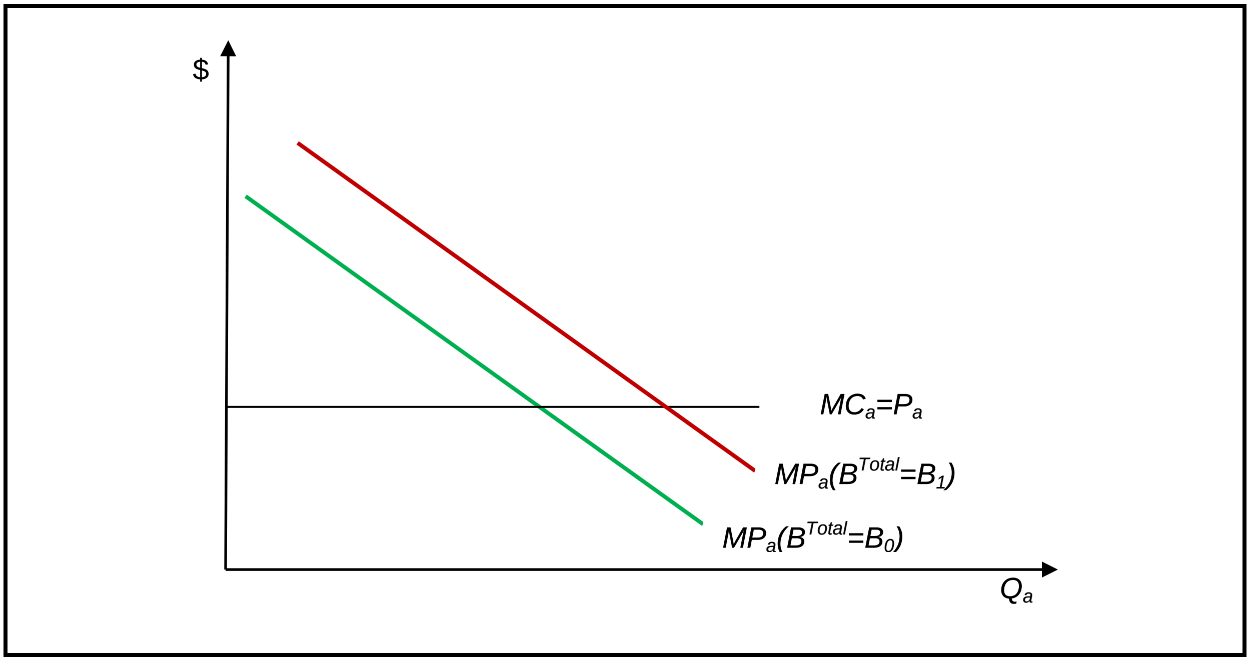
Source: RTI International.

This simple model formalizes what we mean by underprovision. Underprovision results because of the public good characteristics of the CSTI—an individual firm's production of security depends on the total amount of the CSTI in society—and the fact that private firms do not consider the impact of their provision of the CSTI on other firms' ability to produce security. Note that although private firms do provide the public good input (CSTI), they choose a quantity of CSTI lower than the quantity that would maximize security for their given budget. Alternatively, by dedicating more resources to the CSTI (good *B*) and fewer resources to good *a*, they could lower the cost of attaining a given level of security.

3.3 Impact of an Exogenous Increase in the CSTI

Recall that we are assuming that *B* is the CSTI. For the sake of simplicity, we will assume that the level of *B* is fixed at B_0. This allows us to draw a marginal product curve for private inputs, a_i, used to produce cyber security. Initially, with the level of CSTI fixed at B_0, the marginal productivity of a_i can be represented by the functional curve $MP_a(B^{Total}=B_0)$ as in Figure 3-2. If there is an exogenous increase in *B* from B_0 *to* B_1, the marginal product of *a* will increase at all quantities of *a*, shifting the marginal product curve to the right to the functional curve labeled $MP_a(B^{Total}=B_1)$. The key insight from this simple observation is that increased public provision of CSTI will increase the marginal productivity of all private expenditure on cyber security. Each dollar devoted to producing a safe cyber environment will result in an even greater increase in the level of cyber security attained.

Figure 3-2. Marginal Product and Marginal Cost of Production of Cyber Security Inputs



Source: RTI International.

3.4 Rationale for Public Provision of the CSTI

Note that this stylized model does little to help explain why public provision of the CSTI may be preferred. The model suggests that one option could be for a simple subsidy set at the value of I^{i}_{bj} (evaluated at the optimal quantities for B^{Total} and a_j) to provide the proper incentives to the firms to produce CSTI. However, such a scenario is unlikely. Both firms would have to collaborate in the manner of a single entity, sharing R&D outputs while not duplicating any efforts. This would be difficult and costly to coordinate resources and enforce sharing. In contrast, the public sector would have every incentive to disseminate infratechnology and technology platforms freely.

If it is true that the CSTI is better provided by the public sector, then other economic forces must be playing a role. For example, either (1) there are additional/alternative market failures involved beyond the fact that the CSTI, in particular, and technical infrastructure, in general, are public goods, or (2) the public sector has higher productivity in producing the CSTI, in particular, and infratechnologies, in general.[30]

In fact, the reality may be that each of these factors comes into play. Prior NIST retrospective impact studies have found evidence in support of each of these propositions. For

[30] Additionally, it could be that a subsidy for privately provided CSTI would be administratively complex and costly.

example, these studies have found that transaction costs are lowered between independent firms operating at different tiers of supply chains. This is highly suggestive that asymmetric information or uncertainty over input quality has come into play between tiers of a supply chain. For example, nearly half of all NIST retrospective impact analyses have identified transaction cost savings. These savings typically occur between the manufacturers of measurement equipment and the users of measurement equipment. Although manufacturers can claim high degrees of accuracy (high quality), absent NIST standards, their customers devote higher levels of resources to verifying the quality of the measurement equipment they have purchased. This reduction in uncertainty over equipment quality has been identified in studies of laser and fiberoptic power calibration standards, sulfur fuel standards, cholesterol standards, thermocouple standards, and power calibration devices, to name a few of the significant studies. Given that suppliers have adopted NIST technical infrastructure, and customers are aware of this, the customers are assured of product quality or characteristics and can economize on testing and monitoring of purchased inputs.

Additionally, past retrospective impact studies of NIST investments frequently have found that NIST, because of its measurement expertise, can produce infratechnologies at lower cost than private-sector counterparts can. Taken together, this stylized model and the body of past NIST retrospective impact studies provide a better understanding of the role that private and public institutions can play in providing CSTI. When the core problem is related solely to the quasi-public-good nature of the CSTI, the preferred policy may be to subsidize private provision of these quasi-public goods. However, when either multiple market failures are in play (e.g., uncertainty, asymmetric information, or coordination failures) or the CSTI components are closely related to the core expertise of public institutions, public provision of the quasi-public goods may be the preferred policy option.

In the simplest form, a public good that acts as an input in firm production processes does not comprise a sufficient rationale for public provision of the public good. A simple subsidy has the capability of creating the incentive for private firms to privately provide the optimal quantity of the public good. However, when multiple market failures occur in the provision of an input, such as a public good input that suffers from uncertainty, asymmetric information, or coordination failures, the combined aggregate negative effect on investment is sufficient to rationalize public provision of the public good.

4. ANALYSIS METHODOLOGY

This section describes, in detail, the methodology used to estimate economic impacts. In brief, the analysis approach can be segmented into four principal components:

1. Estimation of CSTI spending by public and private sector stakeholders to develop a picture of the annual investment made in the CSTI nationally
2. In-depth, case-study style interviews with private-sector cyber security directors to identify CSTI gaps and develop an instrument for a national survey of security managers
3. Interviews with security experts to identify specific CSTI improvements that could provide at least a 10% increase in cyber security if implemented
4. Economic analysis that quantified the value of narrowing CSTI gaps to U.S. firms

4.1 Estimating Current Spending on Cyber Security Technical Infrastructure

As introduced in Section 2, a variety of stakeholders in the public and private sectors make investments in the CSTI. Relevant government and private-sector investments include those for the development, refinement, maintenance, testing, and evaluation of new data (e.g., threat data); standards; standard processes; tools; or techniques, as well as the coordination of experts and industry members and the development of educational and best-practices materials.

Current spending on the CSTI was estimated for three principal stakeholder groups:

- **Government:** Several different government agencies make investments in cyber security infrastructure R&D through both internal activities (e.g., NIST) and external activities (e.g., technology organizations, research organizations, and academics).
- **Industry consortia, associations, and user groups:** Many private organizations pay for infratechnology development through their involvement in industry associations and consortia such as the Information Systems Security Association (ISSA) and Information Systems Audit and Control Alliance (ISACA). Organizations with a broader focus include the International Organization for Standardization (ISO), and user groups such as OpenID provide a more distributive way in which investments in infratechnology occur.
- **Private organizations:** Individual organizations may develop their own proprietary standards that they use for internal operations and/or impose on their suppliers or customers. For example, Visa led efforts to develop the PCI security standards, now used by most financial institutions, which require businesses accepting their card for payment to implement certain technical solutions, policies, and procedures.

Data on spending by government, industry and user groups, consortia, and other associations came from both primary sources (e.g., informal interviews) and secondary sources (e.g., annual reports, websites, and other documents). Private-sector estimates of labor spent supporting industry association and consortia activities were collected directly from organizations as part of the national, cross-industry Internet survey, as well as indirectly through data reported by industry associations and consortia. The results of this data collection effort are presented in Section 7.

4.2 Identifying Gaps in the CSTI

Gaps in the CSTI were identified during in-depth, case-study style interviews with private-sector cyber security directors in industries expected to be most affected by cyber security spending and losses.

4.2.1 Focus Industry Selection

Focus industries were selected through analysis of secondary data, including IT spending, cyber security spending, cyber security losses, cyber security downtime, consequences to society of cyber security attacks, IT intensity, and employment (see Table 4-1). The principal data sources were two research reports by the consulting firm Gartner, Lovelock et al. (2009) and Wheatman (2010), and the U.S. Department of Justice's Bureau of Justice Statistics' National Computer Security Survey (2008).[31] High per-employee security spending indicates that an industry has a history of frequent attacks, expects more cyber security attacks in the future, or expects high losses from any cyber attack.

Gartner reports provided information on U.S. industries' IT spending and cyber security spending. According to the Gartner report entitled *Dataquest Alert: Utilities, Healthcare and Government Lead IT Spending Growth in Challenging 2009,* the finance, manufacturing, and retail industries spent the most on IT in 2009. Although this information is the best available, the Gartner survey estimates encompass all IT spending and not cyber security spending in particular. Thus, rankings based on this metric alone would be driven more by the size and IT-intensive nature of the industries than by the risk of cyber security threats. However, these numbers are indicative of the potential magnitude of the impact a cyber security attack would have.

Another Gartner report, *2010 Update: What Organizations Are Spending on IT Security,* provided data on cyber security spending per employee. High per-employee security spending indicates that an industry has a history of frequent attacks, expects more cyber security attacks in the future, or expects high losses from any cyber attack.

[31] Data used for 2010 IT spending and cyber security spending are not shown in Table 3-1 based on Gartner's Copyright and Quote Policy, which does not allow data over 12 months old to be quoted.

Table 4-1. U.S. Data on Cyber Security Losses, by Industry

Industry	NAICS (2–6 digits)	Risk Level[a,b]	Monetary Losses per Business[a] (mean, 2010$)	Number of Incidents per Business[a] (mean)	Median Downtime per Business[a] (hours)	Employment[c] (thousands)
Computer system design	5415	Critical	37,821	7.0	16.0	1,252.2
Finance	521–523	Critical	51,666	6.9	12.0	4,184.0
Health care	621–623	Critical	35,191	6.9	15.0	14,303.0
Insurance	524–525	Moderate	43,992	6.4	13.0	2,423.5
Manufacturing	31–33	Critical/High	39,649	7.0	17.8	13,333.4
Publications and broadcasting	511, 515, 516, 519	Critical	33,588	7.4	20.0	1,516.2
Retail	44–45	High	37,927	7.0	22.0	15,515.4
Scientific R&D	5,416–5,417	High	32,095	7.3	20.0	1,460.4
Telecommunications	517–518	Critical	38,576	7.0	20.0	1,251.0
Utilities	22	Critical	27,206	6.9	12.0	637.2
Wholesale	42	High	37,916	7.3	20.0	6,227.4

[a] DOJ Bureau of Justice Statistics (2008). [b] The DOJ study defined risk levels as critical, high, moderate, and low. According to the study methodology report, "[t]hese levels are based largely on whether the industry is part of the U.S. critical infrastructure, as defined by the Information Sharing and Analysis Centers (ISACs)" (Davis et al., 2008, p. 10). [c] U.S. Census Bureau (2007a).

The 2008 DOJ survey provided information from a sample of approximately 3,000 organizations. Included in their summary statistics were information on industries' level of risk (using an ordinal scale), the average monetary losses per business, the average number of incidents per business, and the median downtime per business. The finance industry had the highest reported losses per business, retail had the highest downtime, and the number of incidents did not vary significantly among industries.

Gartner and DOJ data were used to develop a set of scores to rank the industries likely to be most affected by improvements in cyber security. The scores were developed as follows: For each metric, the industry with the highest value was given a score of 1. Each other industry was given a score equal to its value for the metric divided by the highest score for that metric. For example, retail had the highest employment with approximately 15 million employees; thus, it was given the score of 1 for employment. Manufacturing had approximately 13 million employees; thus, it was given a value of 0.86, which is equal to 13 million divided by 15 million. A score of 1 is the highest possible score for each metric.

Six focus industries were selected. As summarized in Table 4-2, four industries—finance, health care, manufacturing, and retail—ranked highly. These same four were defined by a DOJ study to be of critical or high risk to the country should they have a major catastrophe (DOJ, 2008). Manufacturing and retail are both very large industries; thus, the impact of a cyber attack on either industry could have a substantial impact on the overall gross domestic product. Further, the retail industry has large volumes of customer data that are at risk of loss. The finance and health care industries are in possession of even more valuable personal information such as bank account numbers and Social Security numbers.

The final two industries—telecommunications and utilities—were selected because these industries are critical public assets. Internet service providers and other telecommunications providers are directly linked to the cyber security technical infrastructure. Because we did not have data available on cyber security spending by the telecommunications industry, we did not have a score for that metric to contribute to their rankings. It is likely that the industry would have a higher overall score if these data had been available. Utilities were selected because they are at particularly high risk, given their extraordinarily low level of security (ELP, 2008) and because the impact of a successful attack on an electric utility or the electrical grid could have far-reaching impacts on the economy (e.g., ICF, 2003; ELCON, 2004).[32]

[32] Of note, government was not selected because the focus of this study was on private-sector investments in cyber security, which are not largely mandated by government. The federal government does not operate with production constraints similar to those of the private sector; for example, OMB can mandate that all federal government agencies invest in a certain area, regardless of the costs.

Table 4-2. RTI Index Scores Developed for Case Study Selection, by Industry

			Per Business				IT Spending		
Industry	NAICS (2–6 digits)	Risk Level	Monetary Losses	Number of Incidents	Median Downtime	Employ-ment	Total IT Spending	per Employee	Total Score[b]
Manufacturing	31–33	0.88	0.77	0.94	0.74	0.86	1.00	0.30	5.48
Finance	521–523	1.00	1.00	0.93	0.50	0.27	0.63	0.72	5.05
Retail	44–45	0.75	0.73	0.94	0.92	1.00	0.43	[a]	4.77
Health care	621–623	1.00	0.68	0.92	0.63	0.92	0.18	0.30	4.63
Computer system design	5415	1.00	0.73	0.95	0.67	0.08	0.01	0.94	4.38
Insurance	524–525	0.50	0.85	0.85	0.54	0.16	0.36	1.00	4.27
Scientific R&D	5,416–5,417	0.75	0.62	0.99	0.83	0.09	0.01	0.94	4.24
Wholesale	42	0.75	0.73	0.98	0.83	0.40	0.20	[a]	3.90
Publications and broadcasting	511, 515, 516, 519	1.00	0.65	1.00	0.83	0.10	0.28	[a]	3.86
Telecommunications	517–518	1.00	0.75	0.95	0.83	0.08	0.23	[a]	3.84
Utilities	22	1.00	0.53	0.92	0.50	0.04	0.30	0.50	3.79

[a] No source data available. [b] Total score is the sum of the seven indices. Industries in bold were selected for case study.

To focus the discussion and thus improve the representativeness of our interview data collection, we concentrated on a set of sub-industries within the six key industries. In manufacturing, we narrowed our choice to the electronics sector, while in finance we focused on large banks and credit card/payment companies. In health care, we concentrated on hospitals and health systems. In retail, we focused on organizations with a large online presence, and in the telecommunications industry, we looked at Internet service providers. Finally, in the utilities sector, we focused on organizations that transmit and/or distribute electricity.

4.2.2 Case Study Interview Data Collection

Between January and October 2011, RTI conducted 36 in-depth, case-study style telephone interviews with cyber security directors (Table 4-3). Although confidentiality and anonymity were promised to all respondents, it can be reported that the individuals with whom we spoke were generally at the level of director of cyber security (exact titles varied), and each had approximately 10 years of related cyber security experience.

Because the purpose of the interviews was to identify gaps in the CSTI and develop a survey instrument, the interview protocol used for the telephone interviews matured over time as additional information was learned. No single interview guide or survey instrument could encompass cyber security issues across all industry groups. However, as topics and themes relevant to cyber security investment decision making clearly emerged in our interviews, they were incorporated in to the final survey instrument. The following key questions were posed in the interviews:

- **What are organizations currently spending on cyber security?** We elicited information about organizations’ spending on cyber security-related hardware, software, and labor as it relates to explicitly protecting their company, as well as investments made in shared technical infrastructure (e.g., labor and membership fees to participate in industry associations/consortia).

Table 4-3. Number of Case Study Interviews and Survey Pretests, by Industry Group

	Case Study Interviews	Surveys Pretested[a]
Manufacturing	6	2
Finance	8	3
Retail	5	2
Health care	7	1
Telecommunications	5	1
Utilities	5	1
Total	**36**	**10**

[a] Selected parts of the survey instrument were pretested at different points as it evolved over time.

- **What gaps currently exist in organizations' cyber security technical infrastructure?** To seek an answer to this question, we posed questions such as the following: (1) If you had a 10% increase in your cyber security budget, what would you spend it on? Why don't you spend any/more money on this area today? (2) In what areas do you think your spending is least effective (i.e., you're spending too much for the security improvement you gain)? Why is this spending not as effective as you would like?
- **In the future, what foreseeable technical infrastructure gaps may emerge as organizations increase adoption of new technologies, such as cloud computing?** In addition to soliciting technical infrastructure domains in need of development, we asked questions such as the following: What security concerns do you currently see as you look into the future at technologies your company is likely to use—cloud computing/ virtualization, increased use of mobile devices, increased use of social media, etc.? Why are you concerned (i.e., what security infrastructure/solutions are missing as you look forward)?
- **What are the consequences of the identified technical gaps?** We queried the impact in terms of benefits—reduction in excessive redundancy and mitigation costs—and business operations (e.g., delay costs, IP loss). For each gap identified, we asked about the specific impacts in terms of the counterfactual (e.g., If Technical Gap X were removed, how much money would you save? If Technical Gap X were removed, what other benefits would be gained—accelerated production, reduced IP losses?).

4.2.3 Final Technical Gap Selection

During the interviews, nine specific CSTI gaps were identified. These gaps represent the areas in which respondents believed that their existing cyber security level is less than desired and for which technical infrastructure barriers exist[33]:

- Authentication of all system users
- Sharing of or access to threat data
- Specification and collection of security metrics
- Mobile device security
- Cloud security
- Automated threat detection and prevention
- Protection and mitigation from loss of equipment and media
- Education about IT security best practices
- Standards for meeting auditing and compliance requirements.

[33] Note that many of these gaps are similar to the list of "hard problems" identified by DHS (see page 1-5).

Section 6 provides a complete description of each of these gaps, including a discussion of current related CSTI investments.

4.3 Identifying Specific Improvements to Narrow CSTI Gaps

After identifying CSTI gaps, we conducted a set of 25 focused interviews with cyber security experts in the private sector, academia, and government aimed at identifying new CSTI technologies that could improve the cyber security of organizations (Table 4-4). Specifically, we asked security experts to identify new CSTI that could improve security in each of the nine gap areas by at least 10% (as measured by a reduction in current or perceived future incidents and breaches). During our interviews, we probed participants to identify specific types of standards, data-sharing mechanisms, best practice documents, and other protocols that could improve the CSTI in each of the nine areas.

As described in Section 3, improvements in the CSTI will result in either a reduction in total spending on cyber security to achieve the same level of security or an improvement in an organization's level of security with the same level of spending on cyber security, depending on whether an organization is cost minimizing to achieve a specific level of security or security maximizing with a given budget. Section 6 presents a recommended set of CSTI improvements based on the interviews conducted and literature and reports reviewed.

4.4 Estimating Benefits Associated with Improvements in the CSTI

To estimate the economic impact of narrowing gaps in the CSTI, we developed a set of conceptual equations describing benefits from an improved CSTI and then developed survey questions that would allow us to quantify these benefits. Based on feedback received during the case study interviews with industry,[34] we developed a two-stage approach to estimating benefits. First, we interviewed security experts to identify CSTI improvements that would deliver a 10% improvement in cyber security for U.S. organizations. Second, we estimated organizations' willingness to pay for a 10% improvement in cyber security through a national survey.

Table 4-4. Number of Security Expert Interviews

	Interviews
Consultants	10
Government	8
Academia	3
Nonprofit	4
Total	**25**

[34] During the case study interviews, industry representatives were consistently unable to quantify the benefits of specific CSTI improvements and the associated benefits.

4.4.1 Economic Analysis Framework—Using a Willingness-to-Pay (WTP) Approach

Conceptually, a comprehensive measure of the economic benefits associated with narrowing gaps in the CSTI includes both cost reductions and quality improvements. Specifically, it includes any reduction in current cyber security-related spending plus the economic value associated with any increase in the level of cyber security minus the adoption costs associated with using any new CSTI technologies:

$$\textbf{Industry benefits} = \sum \Delta \text{ reduced spending on cyber security} + \left(\sum \Delta \text{ benefits of increased cyber security} - \sum \text{adoption costs}\right)$$

The benefits of increased cyber security can include several factors but primarily consist of a reduction in direct losses associated with cyber attacks (e.g., financial losses) and/or a reduction in delays/opportunity costs (e.g., staff productivity, product quality, and reputation/customer losses). However, our interviews indicate that IT security managers focus on what they know when considering the benefits of IT security investments; they were unable to quantify the full impact of IT security on non-IT staff productivity, product quality, and potential customer losses. Thus, our approach for data collection focused on developing estimates of benefits in terms of cyber security cost reductions.

The following is a list of the primary types of excessive cost categories that IT security managers generally think about when making investments:

- Time spent on redundant activities
- Time spent on mitigation activities
- IT operations delay
- Capital spending on redundant systems
- Capital spending on mitigation activities

Given that the estimated benefits are not inclusive of non-IT-related costs savings and quality benefits, data collected likely represent a significant underestimate of the total benefits of improvements in the CSTI.

During our interviews, participants were unable to estimate the potential benefits of improvements in cyber security at a granular level. However, when presented with an unknown "product or service" that could improve their security by a certain percentage, measured in terms of the number of incidents experienced each year, participants were able to provide an annual willingness-to-pay estimate. Therefore, to estimate the benefits to organizations for reducing the size of the CSTI gap, we used the survey to pose the following key question:

WTP Question 1. "How much would you [your organization] be willing to pay for a 10% improvement in your IT security effectiveness, as measured by the number of incidents you experience each year?"

Responses were used as an estimate of the benefit that the organization would receive in terms of reduced spending on cyber security. This is referred to as a contingent valuation estimate.[35] Although contingent valuation does not allow disaggregated estimation of benefits (e.g., cost savings in terms of IT staff labor), there are several primary advantages of contingent valuation for quantifying the benefits of an improvement in cyber security as a result of narrowing CSTI gaps:

1. *Full value can be assessed efficiently and effectively*. When determining how much companies would value an improvement in cyber security, each respondent was asked to consider and account for all the ways that an improvement in cyber security would benefit their organizations in terms of cyber security cost reductions. As a result, this willingness-to-pay estimation approach measured the value that cyber security managers place on CSTI technologies. This approach also implies that asking questions in this manner is more efficient because it is less likely that important benefits will be left out.
2. *Monetization is simple and defensible*. Because the respondents' answers were already reported in terms of dollars, there was no need for secondary data to monetize the benefits metrics estimated by cyber security managers. This reduced the data collection and analysis time and also reduced inaccuracy in final estimates that may have resulted from making assumptions based on secondary data are most appropriate for particular monetization tasks.
3. *Cyber security managers were most comfortable with a willingness-to-pay approach*. Early pilot tests revealed that WTP questions were the easiest for cyber security staff to answer, primarily because they allowed staff to use their own methods for mentally estimating the value of an improvement in cyber security. As a result, respondents were not required to consider what they would do without an improvement. Instead, they could estimate the benefits they received by thinking about the costs they saved, for example.

It is important to recognize that the contingent valuation or willingness to pay approach has limitations that cannot be controlled for. For example, specific benefit characteristics and adoption costs cannot be broken out using this method. Further, survey respondents may not have thought about, or be aware of, all of the potential benefits when providing their estimates.

[35] Contingent valuation is a survey technique that is well established for nonmarket valuation (estimating the monetary value of items that are not part of a market). Continent valuation has been used extensively in environmental studies – e.g., to determine the economic value of clean air (Champ et al, 2003). Contingent valuation has also been used to assess demand for new products and services (Braden et al, 1997), and recently, to estimate the benefits of government-provided technology infrastructure (Rowe et al, 2010).

In the case of estimating the benefits of improvements in the CSTI, the advantages of willingness-to-pay-based estimation outweigh the approach's limitations. In particular, some survey respondents and interview participants may not have been able to accurately gauge how much they would have been willing to pay for an improvement in the CSTI, and some survey respondents were unwilling to provide estimates. These limitations are shared by all surveys to some degree, because survey results are only useful to the extent that respondents are willing and able to provide truthful and accurate responses to the questions being asked.

To complement the initial willingness-to-pay question, respondents were shown the list of nine key gaps and asked to indicate the percentage of the new money they would apportion to each area. We asked this question:

> **WTP Question 2. "If your [your organization's] IT security budget increased by 10%, how would you spend the additional dollars if you had to allocate them among the activities and processes listed above?"**

The responses to this question demonstrate respondents' prioritization of activities and show how much of additional budget dollars they would want to spend on the nine outlined activities compared with other activities. Respondents' spending priorities were used to deduce their willingness to invest in each of the nine areas.

4.4.2 Survey Data Collection

The survey targeted at cyber security managers was fielded between November 2011 and February 2012 with the support of several cyber security consortia and industry associations. (See full survey instrument in Appendix A.) Table 4-5 lists the 162 survey respondents by industry group. A more comprehensive breakout of the survey response is available in Section 7.

Table 4-6 lists and describes the organizations through which our survey instrument was disseminated. In all, approximately 116,900 subscribers were reached via newsletters (including some international organizations), and approximately 18,000 users were reached via direct e-mail (all U.S.-based). The highest responses correlated with direct e-mailing efforts,[36] and we estimate that roughly 75% of survey takers were responding to a direct mailing. Thus, we can estimate the response rate of our direct e-mailing efforts to be approximately 1.2%.

[36] The newsletters that were sent out tracked responses through an intermediary link, allowing us to broadly ascertain the response rate resulting from direct e-mail outreach as opposed to through newsletters.

Table 4-5. Number of U.S. Survey Respondents, by Industry Group

	Survey Reponses
Manufacturing (electronics)	17
Financial	34
Health care	13
Retail	6
Telecommunications	24
Utilities	11
Other	57
Total	**162**

Table 4-6. Organizations that Disseminated the Survey Instrument

Organization	Brief Description	Number of Members
Information Systems Audit and Control Alliance (ISACA)	Global industry association that offers training and certification in information systems auditing, security, and control	Approximately 95,000 members reached via newsletter, and 70 member organizations reached via direct e-mailing
North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)	Regional consortium representing various sectors in the health care industry with the goal of promoting health care IT and driving standards	Approximately 1,500 members reached via newsletter
National Electronic Manufacturers Association (NEMA)	Industry association of manufacturers of electrical products. Promotes the development of industry standards, advocates industry policies, and provides data analysis.	Approximately 20,000 members reached through e-magazine
Financial Services Information Sharing and Analysis Center (FS-ISAC)	Organization responsible for sharing information about physical and cyber security threats and vulnerabilities affecting financial services companies	333 contacts reached through direct e-mailing
International Data Group (IDG)	For-profit company that, among other functions, maintains a contact list of opted-in subscribers to various magazines, including information-security-themed publications	Approximately 18,000 subscribers reached through direct e-mailing
Network World	Electronic magazine publishing Internet-related news	Tens of thousands of subscribers reached via newsletter

The survey instrument included several types of questions aimed at better understanding cyber security investments:

1. Respondent profile (Questions 1 through 10, 12, and 13, and Questions 21 through 25)
2. Percentage of cyber security spending that is proactive or reactive (Question 11)
3. Cyber security costs (Question 14)
4. Mobile and cloud computing (Questions 19 and 20)
5. Impact of improved CSTI (Questions 15, 16, 17, and 18).

The first category of questions is specific to the characteristics of the responding organization and to its cyber security incidents. The second category investigates cyber security spending as occurring along a spectrum from proactive investments to avoid incidents and breaches to reactive investments made in response to incidents and breaches.[37]

The third category of questions is related to the allocation of an organization's cyber security costs among the predefined activities and processes. Question 14 explicitly addresses gaps in terms of the proportion of an organization's cyber security budget associated with a relevant activity.

The fourth category is composed of questions specific to mobile devices and cloud computing; these questions were asked to augment our findings given the prevalence of industry comments about these platforms. Question 19 asks about the impact of a hypothetical guarantee on mobile device security on the number of such devices being used. The potential growth of cloud computing with guaranteed security is considered in Question 20.

Finally, the fifth category of questions was included to help inform the public sector about how it allocates its scarce resources in support of advancing cyber security in the private sector.

Question 15 asks organizations to estimate their willingness to pay for the improvement in security. As described above, this question's design was based on a contingent valuation methodology to help elicit an estimate of the benefits of an improvement in cyber security based on organizations' hypothetical willingness to invest. Question 16 addresses the reactive piece of this benefit estimate by asking organizations specifically how much they could reduce reactive spending if their level of security increased.

[37] RTI introduced this concept into the cyber security conversation in earlier studies (e.g., Gallaher, Link, and Rowe, 2008), and over time has found that organizations' proclivity to be more proactive versus reactive in cyber security investments is correlated with other internal activities, such as the department in which such decisions are made (i.e., usually either in the IT department or the risk management department).

Question 17 asks how an organization would allocate an exogenous increase in its cyber security budget among the activities/processes listed above, everything else remaining constant. This question was constructed to determine the activity(ies)/process(es) that the organization underinvests in in a relative sense. Accordingly, if the public sector's involvement in enhancing cyber security is based on the premise of market failure, and if the role of the public sector is to identify barriers that inhibit private-sector investment from occurring at a socially desirable level, then barriers must exist in those areas in which the private sector underinvests.

Question 18 addresses this same concept, but asks the question differently.[38] Specifically, it asks about the percentage increase in the organization's cyber security budget required if the organization could exogenously become more effective in achieving each of the activities/processes listed above. Responses to this question might indicate activity(ies)/process(es) in which a marginal dollar would be most effective. Those are, therefore, the areas where public-sector attention might be focused.

4.4.3 Calculating National Economic Impact Estimates

The benefits of narrowing the size of the nine gaps in the CSTI for all U.S. organizations were calculated through several steps, relying upon original data collection as well national statistics and other publicly available data. As described further in Section 7, we used a weighted average (using organizational revenue) of willingness to pay for each improvement in the CSTI to build up our estimates. To account for differences in industries, we further weighted the industry-based willingness-to-pay estimates by using Garter data on IT intensity—i.e., the percentage of revenue each industry spends on IT capital and labor (2002).

The following equations show how we extrapolated to national- and industry-level impact estimates. First, we calculated how much each survey respondent *k* was willing to pay for each of the nine CSTI improvements *j*, as follows:

$$\boldsymbol{WTP_{ijk}} = WTPS_{ik} \times CSTI\%_{ijk}$$

where

$WTPS_{ik}$ = each respondent's stated willingness to pay for a 10% improvement in overall cyber security (in response to Question 15 in the survey)

$CSTI\%_{ijk}$ = each respondent's stated allocation of a 10% budget increase by CSTI_i (in response to Question 18 in the survey)

Based on the survey data, we calculated each respondent's willingness to pay for CSTI per dollar of revenue (as stated for their company). Next, for each CSTI improvement, we

[38] During the pretesting of the survey instrument, we found that some organizations could answer one of these questions (Questions 17 or 18) more easily than the other. Both are included on the survey for completeness.

calculated the average willingness to pay across all respondents. We then extrapolated this to the industry level using industry revenues (using data from the U.S. Census Bureau [2007b]) weighted by each industry's relative IT intensity (using data from Gartner [2012]). For each industry i, an estimate of the benefits of each of the nine CSTI improvements (j) was calculated as follows:

$$\textbf{Benefits}_{\boldsymbol{ij}} = WTPR_j \times revenue_i \times \frac{IT\ intensity_i}{Avg.IT\ Intensity}$$

where

$WTPR_j$ = average respondent willingness to pay per dollar of revenue for CSTI improvement *j*

revenue$_i$ = revenue for industry *i*

IT intensity$_i$ = IT spending/revenue for industry *i*

4.4.4 Limitations of the Benefits Estimation

The approach for benefits estimation had several key drawbacks, and as a result, the benefits estimates calculated are likely an underestimate. First, only IT-related cost savings were calculated. The benefits associated with reduced additional direct and indirect losses associated with cyber security mitigation efforts and losses outside of the IT enterprise were not calculated. Such losses include financial losses as well as delay/opportunity costs such as reduced non-IT staff productivity, reduced product quality, and reduced reputation/customer loss.

A 2008 study by McAfee estimated that computer crime costs companies around the world over $1 trillion a year as a result of leaked data, remediation costs, and reputational costs; specifically, the report estimated that $559 million in annual losses resulted from intellectual property loss.[39] Although the accuracy of such estimates is highly questionable,[40] the significant economic impact of the non-IT losses associated with inadequate cyber security is widely supported.

Second, this analysis estimated the benefits of only a 10% increase in cyber security that occurred only as a result of new CSTI. While experts suggest that it would be impossible to completely prevent all cyber security attacks[41], improvements beyond 10% are potentially feasible. A 2012 study sponsored by Bloomberg and Ponemon estimated that the cost for the set of 172 companies interviewed to increase their security to a level that would thwart 95% of attacks would be approximately $46.6 billion per year (Domenic and Afzal, 2012). Currently,

[39] See http://www.mcafee.com/us/resources/reports/rp-unsecured-economies-report.pdf.

[40] See for example Greenberg (2012) and Florencio and Herley (2011).

[41] See Schneier (2012).

these companies spend $5.3 billion per year to achieve an estimated 69% rate of successful attack prevention. If improvements in the CSTI could enable more than a 10% increase in cyber security, this earlier result suggests that our estimates understate IT-related benefits (cost savings) associated with improving the CSTI.

Third, the willingness-to-pay approach may have limited the benefits that were estimated. Although past research has suggested that respondents to such contingent valuation questions sometimes overestimate (Loomis, 2011), in this case, it is likely that the estimates provided in this study are low. During scoping discussions before the survey and follow-up interviews with several survey respondents after they completed the survey, several security managers indicated that they found it difficult to complete the willingness-to-pay questions and as a result they likely underestimated their willingness to pay.

5. CURRENT SPENDING ON CYBER SECURITY TECHNICAL INFRASTRUCTURE

This section is devoted to the review of what we estimate to be $716.1 million in total CSTI-related activity for 2012. This estimate is based on records from the FY2012 U.S. Government budget, Internal Revenue Service (IRS) filings from consortia, and survey data from private firms.

The federal government was the largest contributor at 70.79% of total CSTI funding ($506.9 million), followed by industry consortia at 9.29% ($66.5 million), and private firms at 19.93% ($142.7 million). Federal agencies such as DHS, NIST, and DoD have national mandates to provide computer security (NITRD, High Performance Computing Act of 1991). But standardized operating protocols and data exchange paradigms require coordination among private-sector firms to be effective. Thus, industry consortia like ISACA and the Internet Society develop methods, techniques, and standards for ensuring cyber security and are critical CSTI investors.

The documentation of CSTI funding is subject to uncertainty. An exhaustive review of budget documents for federal agencies, IRS filings for industry consortia, and survey data for private-sector firms was performed to identify CSTI-related spending. Yet, data were not labeled explicitly as CSTI expenditures, thereby requiring the applications of the definitions from Section 2 to public and private program goals, activities, outcomes, and services. The best available data were FY2012 federal data, 2009 to 2010 IRS filings for industry consortia and nonprofit organizations, and survey data from 2010. Comparable single-year data were not available. Thus, the estimate for 2012 assumes that industry consortia and private firm costs were at least what they were in 2010.

5.1 Federal CSTI Spending

The U.S. federal government funds technical infrastructure research to ensure that the United States and its citizens can take advantage of the information technology revolution (White House, 2009). To identify federal spending, budget justification documents on funding of individual programs were obtained and analyzed within each of the aforementioned government agencies. Any program with “cyber,” “information security,” “IT security,” or similar term in the title or description was considered potentially relevant. Then, the descriptions and supporting materials were evaluated to determine which programs are dedicated to developing CSTI as defined in Section 2. Budget requests for individual agencies’ operations (such as using technology to achieve a security goal) and programs that are specific to an individual agency’s agenda (e.g., programs aimed at developing technologies for the government to use to thwart cyber criminals) were not considered CSTI spending.

Five federal agencies have major programs that fund research, development, testing, evaluation, and coordination of technical infrastructure activities for broader use by the public and private sectors. These include DoD, DHS, NSF, Department of Energy (DOE), and NIST (Table 5-1). These agencies' CSTI efforts are coordinated to some extent by the federal NITRD. The following sections detail each relevant agency's CSTI funding requests for FY2012. These sections provide general overviews of the agencies and descriptions of the relevant programs, including the rationale for characterizing each program as CSTI-related.

5.1.1 Department of Defense

DoD funds the CSTI extensively under its Research, Development, Test & Evaluation (RDT&E) account. The DoD base budget (not including overseas operations) was $553 billion for FY2012, and the budget for RDT&E was $75 billion (Comptroller, 2011). The budget for the CSTI was estimated at $212.5 million. Thus, DoD funding accounted for about 41.93% of total federal CSTI spending. DARPA, OSD, Defense information Systems Agency (DISA), Army, and Air Force all have RDT&E programs funding CSTI. The balance of this section describes the programs the rationale for their inclusion as CSTI investment.

5.1.1.1 Defense Advanced Research Projects Agency

DARPA funds cyber security as part of ensuring U.S. military technological superiority and national security (DARPA, 2012). Often collaborating with other government agencies and universities, DARPA has contributed and continues to contribute to the development of technologies that are widely adaptable and used, such as the Internet and global positioning systems.

DARPA conceptualizes and executes R&D projects to develop interdisciplinary, crosscutting, and convergent cyber technologies (DARPA, 2012). It funded 15.33% of all federal CSTI spending in 2012. DARPA's 2012 total budget was $3 billion (DARPA, 2011). Of this, $77.7 million was devoted to the CSTI under the rubric of basic and applied research, advanced technology development, and management support projects that promote technical infrastructure (DARPA, 2011).

Basic and Applied Research

- *Crowd Source Cyber* ($16.6 million) is considered infratechnology and technology platform research because it develops technology that reduces the risk of coding errors, which are the cause of many security vulnerabilities in software systems. Specifically, it develops an environment that facilitates the mapping from a code/formal specification to the relevant components of a simulation.
- *Resilient Networks* ($20 million) creates routing and switching software that is agile and responsive to threats. It produces technologies to address vulnerabilities in the networking protocols of homes, small businesses, enterprises, and wide-area networks.

Table 5-1. Estimated Federal CSTI Spending (2012)

	Budget ($ million)		CSTI Percentage of Department's Budget
Agency	**Total**	**Estimated CSTI**	
Department of Defense (DoD)*	553,000	212.5	0.038
Defense Advanced Research Projects Agency (DARPA)	3,000	77.7	2.589
Office of the Secretary of Defense (OSD)**	4,649	115.7	2.489
Army	144,900	11.8	0.008
Air Force	149,000	7.4	0.005
Navy	161,400	—	—
Department of Homeland Security (DHS)	57,000	170.0	0.298
Department of Energy (DOE)	29,500	30.0	0.102
National Science Foundation (NSF)	7,800	16.0	0.205
National Institute of Standards and Technology (NIST)	1,000	78.3	7.834
Total	**648,300**	**506.9**	**0.078**

Note: Sums may not add to totals due to independent rounding. * Although DoD includes DARPA, OSD, Army, Air Force, and Navy spending, these five subgroups do not add up to the DoD as additional spending was attributed to the DoD itself. **OSD total budget is the sum of procurement, Research, Development, Test & Evaluation (RDT&E), and operations and maintenance funding.
Sources: NIST (2011a), NSF (2011), DOE (2012), DHS (2011a), OSD (2012), DARPA MJ (2011).

- *Cyber Situational Awareness and Response (CSAR)* ($17.5 million) develops techniques to exploit data from events on host and networks. It falls under the rubric of infratechnology because it advances attack and attacker detection, characterization, and assessment techniques.
- *Cognitive Computing* ($12 million) develops technologies that enable computer systems to learn, reason, apply knowledge, and respond to new and unforeseen events. It contributes to cyber threat defense, removes the potential for human errors, and makes personnel more efficient.

Advanced Technology Development

- *Cyber Insider Threat (CINDER*) ($12 million) develops tools and techniques that characterize user missions in a security environment to mitigate threats from insiders. This is considered to be infratechnology funding because it develops techniques to counter threats to networks and systems.

Management Support

- *Cyber Security Initiative* ($10 million) develops a persistent and cost-effective cyber testing environment. This test range was characterized as infratechnology because it enables experimentation of software and hardware in support of assessments of cyber security research and development programs. Furthermore, the program became available for leverage or use by all federal government organizations during 2012.

5.1.1.2 Office of the Secretary of Defense

OSD provides the Secretary of Defense with the necessary staff and resources for policy development, planning, resource management, fiscal, and program evaluation responsibilities. OSD funds infrastructure technology under advanced technology development and promotes agency and public/private cooperation and collaboration. The defense-wide OSD budget was $4.6 billion for 2012 (OSD, 2012), of which $115.7 million was allocated to CSTI. OSD's funding accounted for about 22.83% of total federal spending on the CSTI.

Advanced Technology Development

- *Combating Terrorism Technology Support* ($77 million) to develop, apply, and deploy models and tools to interpret data streams. This is infratechnology development because the focus is on developing models to interpret complex data streams. It can also be considered technology platform development because it builds analytical systems for interagency intelligence and operational communities.
- *Smart Power Infrastructure Demonstration for Energy Reliability and Security* (SPIDERS) ($1.5 million) is focused on proof-of-concept cyber-secure "smart" micro-grids with demand-side management and integration of renewable energy and storage on military installations, in partnership with DOE and DHS.
- *Computer Adaptive Network Defense-in-Depth* (CANDID) ($3.8 million) supports infratechnology for the integration of Virtual Secure Enclaves (VSEs) inside existing tactical networks to enable network defense and ensure command and control.[42]
- *Network Management Tools and Analysis* ($4.8 million) develops standards and tools for policy and measurement-based tactical network management. The project is jointly executed by the Navy, Air Force, and Army, all of which are pursuing technology transition agreements.
- *Software Engineering Technical Practices—Networked Systems Survivability Program (NSS)* ($6.2 million) promotes both infratechnology and technology platform development because this research identifies, develops, matures, and transmits new technologies, system development, and management practices that enable trust and confidence in information and communication technology. This research is conducted with universities (particularly Carnegie Mellon), and some prototypes are tested by other government agencies, such as the Army.
- *Software Engineering Technical Practices—Research Technology, and System Solutions Program (RTSS)* ($13.3 million) provides technical foundations, methods,

[42] This funding is contingent on congressional appropriation and congressional notification.

practices, and solutions that enable assured and flexible system capabilities. It also creates, matures, pilots, and transitions technical foundations and practices for developing and evolving acquisition systems.

- *Software Engineering Technical Practices—Software Engineering Process Management Program (SEPM)* ($1.6 million) researches and publishes models, results, and heuristics for use in analysis diagnostics, feasibility studies, risk evaluation, and early warning indicators in DoD acquisition systems. This is infratechnology development because it provides guidance and expertise in measurement and analysis.
- *Software Producibility Initiative* ($7.4 million) is infratechnology and platform development funding because it develops prototypes, interface formalisms, models, simulation environments, theories, and algorithms to improve software-intensive systems. This research is conducted by universities and various government facilities.

5.1.1.3 Army

The U.S. Army devotes significant funding to RDT&E but a relatively small amount to CSTI activities. The Army had a base budget of $144.9 billion in FY2012, of which $9.6 billion was devoted to RDT&E and $12 million went toward the CSTI (Army, 2011). Thus, the Army funding accounted for about 2.33% of federal CSTI spending. The Army CSTI funding generally develops methods for addressing cyber threats under Army Advanced Technology Development and RDT&E Management Support:

- *Information Assurance* ($8.5 million) matures and demonstrates cyber security technologies that create nontraditional methodologies for defending wireless networks.
- *Continuing Engineering Manufacturing and Development (EMD) for Network Exploitation Test Tools (NETT)* ($3.3 million) portrays evolving hostile and malicious cyber threats. This is infratechnology because it provides open-source/open-method exploitation tools.

5.1.1.4 Air Force

The Air Force has greater funding under RDT&E than does the Army, but less for CSTI. In the base budget of $149 billion, $27.7 billion was dedicated to RDT&E, and $7.4 million went to the CSTI (Air Force, 2011).[43] The Air Force's funding accounted for about 1.46% of federal CSTI funding. Funding mostly goes toward the development of forensic tools, metrics, and other techniques for mitigating cyber threats.

[43] The Navy has a base budget of $161,400 billion; $18,000 billion goes toward RDT&E, but no programs fall within the scope of technical infrastructure (Department of the Navy, 2011).

Air Force Operational Systems Development

- *Cyber Forensic Tools* ($1.9 million) develops metrics for information assurance, secures coalition information-architecture data management, secures collaboration and visualization, and analyzes cyber security bots.
- *Cyber Threat Recognition* ($1.5 million) develops information assurance metrics and an integrated airborne network security information operations platform.
- *Cyber Threat Attribution* ($1.6 million) creates risk mitigation techniques for wireless networks and systems and dynamic policy enforcement and computer/net attack attribution efforts.
- *Digital Forensic Tools* ($2.0 million) are used for development, testing, and evaluation applied to digital evidence processing and computer forensic analysis. This is considered technology platform funding because it develops software tools that increase the probability of data recovery for the government, universities, and private industries.
- *Forensic Technology Gap* ($0.3 million) identifies digital forensic gaps, researches potential solutions, and develops tools to address the gap. This is a collaborative effort with law enforcement/counterintelligence and cyber communities.

5.1.2 Department of Homeland Security

One of DHS's six integral missions is *safeguarding and securing cyberspace*. This means collaborating with industry and various levels of government to "analyze and reduce cyber threats and vulnerabilities; distribute threat warnings; and coordinate responses to cyber incidents to ensure that computers, networks, and cyber systems remain safe" (DHS, 2011b). Investing in the CSTI is a component of accomplishing this mission.

For FY2012, DHS requested $57 billion in funding. Of this, approximately $500 million was dedicated to cyber security, and of that, an estimated $170 million for CSTI (DHS, 2011a). DHS's funding accounted for 33.54% of federal CSTI spending. The funding promotes cooperation between entities and facilitates the dissemination of cyber security information.

Within DHS, the National Protection and Programs Directorate (NPPD) and the Science and Technology Directorate (S&T) fund programs dedicated to infrastructure technology.[44] One of the five missions of the NPPD is to protect and strengthen the U.S. cyber and communications infrastructure. Several programs are aimed at CSTI:

[44] The *DHS Fiscal Year 2012 Budget in Brief* provides descriptions of highlighted programs within each directorate of the DHS. The *Budget in Brief* is the main source for this analysis of DHS funding; yet, to ensure that no programs relevant to CSTI were missed, the *full budget justification* was also reviewed.

- *U.S. Computer Emergency Readiness Team (US-CERT) Operations* (FY2012 $80.9 million) enables US-CERT to improve cyber analytics, cyber security indications and warnings, collaboration and coordination, and cyber incident response. This fund, which focuses on information creation, analysis, and dissemination, is considered infratechnology.
- *Critical Infrastructure Cyber Protection & Awareness* (CICPA) ($61.4 million) supports control systems security and cyber security evaluations. CICPA will work to enhance cyber system security through expanded on-site threat and vulnerability assessment (including extensive work with the private sector). This is considered infratechnology because it focuses on information creation, analysis, and dissemination.
- *Software Assurance and Supply Chain Risk Management* ($9.7 million) allows NPPD to work with software manufacturers, stakeholders, and federal partners to improve security in software development and acquisition. This is considered infratechnology funding because it develops methods and provides direct support to industry and government.

The S&T aims to improve homeland security by working with partners to provide cutting-edge technology and solutions. One program funds CSTI. *Cybersecurity Research* ($18 million) supports cyber security R&D projects such as Cyber Economic Incentives, Moving Target Defense, Tailored Trustworthy Space, and Transition to Practice. This funding falls well within the scope of infratechnology because it develops core concepts and strategy.

5.1.3 Department of Energy

DOE invests in the CSTI to protect and ensure reliable power systems and supply. Of the $29.5 billion requested by DOE in FY2012, approximately $216 million went to cyber security overall[45] and $30 million went to CSTI through Electric Delivery and Energy Reliability/Research and Development (DOE, 2011). This DOE funding was about 5.92% of federal CSTI spending.

Cyber Security for Energy Delivery Systems ($30 million FY2012) enhances the reliability and resilience of the U.S. energy infrastructure by reducing the risk of energy disruptions due to cyber attacks. Under this infratechnology initiative, DOE, in collaboration with energy owners and operators, is developing a technology strategy to secure business IT computer systems and networks.

5.1.4 National Science Foundation

NSF funds R&D in cyber security infrastructure to catalyze the development of technologies to keep the United States secure. The total budget request was $7.8 billion in 2012;

[45] Cyber security funding includes $30 million for *Cyber Security for Energy Delivery Systems*, $22 million for *Cyber Security and Secure Communications*, and $164 million for Cyber Security Safe Guards and Security.

$157 million was dedicated to cyber security, and $16 million to for CSTI in particular (NSF, 2011).[46] This $16 million accounted for 3.16% of the federal CSTI budget.

The NSF budget breaks down research and related activities funding by division or office. Funding for infrastructure technology is overseen by the Office of Cyber Infrastructure (OCI). OCI promotes research, development, and acquisition of cyber infrastructure (Rollup, OCI-1). It requested $16 million for FY2012 to support the Comprehensive National Cybersecurity Initiative (CNCI). This funding promotes technology platform development because it is used to deploy and test cyber security prototypes. It also sponsors infratechnology because it develops experimental approaches, cyber security in advanced computer environments and IT services, and virtual organization and coordination.

5.1.5 National Institute of Standards and Technology

NIST applies IT research, standards expertise, and background on industrial collaboration to improve the security and interoperability of U.S. cyberspace infrastructure. The total NIST budget was $1 billion for FY2012; $78.34 million of NIST's budget went toward the CSTI (NIST, 2011a).[47] NIST's CSTI funding accounted for 15.45% of federal CSTI spending.

The *NIST Cyber Security Center of Excellence* ($10 million) creates infratechnology by bringing together industry, government, and academic experts to develop and accelerate the dissemination of practical approaches for addressing security threats. This public-private collaboration "enhances trust in U.S. IT communications, data, and storage systems; lowers risks for companies and individuals using IT systems; and encourages development of innovative job-creating cyber security productions and services" (NIST, 2012a).

Within NIST's 2012 budget request, the budget for *Ensuring a Secure and Robust Cyber Infrastructure* noted several proposed increases in CSTI funding:

- *Scalable Cybersecurity for Emerging Technologies and Threats* (+$14.9 million FY2012) is included as infratechnology because it develops security techniques, supports security standards, increases the interoperability and usability of security technologies, and accelerates the secure adoption of information technologies.
- *National Program Office for the National Strategy for Trusted Identities in Cyberspace (NSTIC) and the NSTIC Grant Program* (+$24.5 million) coordinates a

[46] The $120 million of the NSF cyber security funding is under the Directorate for Computer and Information Science and Engineering (CISE). CISE cyber security funding is not well documented and it is possible that a fraction of the funding is dedicated to CSTI.

[47] The NIST total CSTI estimate is likely a slight overestimate. The estimate comprises $68.34 million for *Ensuring a Secure and Robust Cyber Infrastructure* and $10 million for *Cyber Security Center for Excellence*. One program, the *National Initiative for Cybersecurity Education (NICE),* under *Ensuring a Secure and Robust Cyber Infrastructure*, is not in the scope of the CSTI. However, although the 2012 funding increase ($4 million) for *NICE* was excluded from our estimate, we found no indication of the program's base funding.

national strategy to improve privacy and security of online transactions. This is infratechnology funding because it develops standards, technologies, and mechanisms for interoperable authentication methods with the private sector and other federal agencies.[48]

5.2 Industry Associations and Consortia CSTI Spending

Numerous private organizations carry out research and provide valuable contributions to the CSTI. They exist to bring together professionals from across organizations with the aim of carrying out technology or policy research, providing precompetitive services, offering education, coordinating activities, and convening discussions (Table 5-2). The purpose is to serve many firms or entire industries through aggregated human capital and collective insight.

Table 5-2. Industry Association and Consortia Contributions to the CSTI

Organization	Tools	Information Sharing	Coordination	Education	Methods, Techniques, and Best Practices	Standards	Training and Certification	Policy and Strategy Research	Other Cyber Security Services
Armed Forces Communication & Electronics Association			●	●					
Center for Applied Identity Management Research			●		●				
Center for Internet Security, Inc.		●				●	●		●
Cloud Security Alliance				●	●		●		
Electronic Devices and Systems for Defense & Security Association Inc.	●								
Energy Sector Security Consortium Inc.		●	●						
Federation for Identity and Cross-Credentialing Systems						●			
Financial Services ISAC	●	●	●				●		
Forum of Incident Response and Security Teams		●	●	●					
Industry Consortium for Advancement of Security on the Internet	●				●	●			●
Information Card Foundation						●			
Information Security Summit			●	●			●		
Information Systems Audit and Control Association Inc.	●		●	●	●	●	●		
Information Systems Security Association				●	●		●		
Information Technology ISAC		●	●					●	

(continued)

[48] Note that funding amounts under *Ensuring a Secure and Robust Cyber Infrastructure* are not full program budgets, only increases to the budgets for FY2012.

Table 5-2. Industry Association and Consortia Contributions to the CSTI (continued)

Organization	Tools	Information Sharing	Coordination	Education	Methods, Techniques, and Best Practices	Standards	Training and Certification	Policy and Strategy Research	Other Cyber Security Services
Institute of Electrical and Electronic Engineers			●	●	●	●		●	
International Information Systems Security Certification Consortium				●					
Internet Society				●	●	●			
Kantara Initiative				●	●	●			
National Cyber Forensics and Training Alliance		●							●
National Cyber Security Alliance				●					
National Defense Industrial Association		●	●	●				●	
North Carolina Healthcare Information and Communications Alliance, Inc.			●	●					●
Online Trust Alliance		●		●	●	●			●
Open Information Security Foundation	●								
OpenID						●			
Organization for the Advancement of Structured Information Standards						●			
Real Estate ISAC		●	●						
TechAmerica Foundation			●	●				●	
United States Cyber Consequences Unit				●					
WaterISAC	●	●	●	●					

For example, organizations may share threat data that is targeted against firms within an industry, as is the case with various ISACs. They may also be responsible for policy research, such as with the Internet Society, which organizes discussions, debates, and papers on the security of the Internet, among other Internet issues. Organizations may also invest in developing technical standards, as is the case with the Internet Society's subsidiary, the IETF (which develops the Internet backbone), the Cloud Security Alliance (which develops cloud computing security standards), and the OpenID Foundation and Kantara Initiative (which develop identity management standards). The Information Systems Audit and Control Association (ISACA) provides professional certification to cyber security managers and executives to ensure that they will employ the best practices in their respective organizations.

Organizations for which cyber security was a prominent goal or issue were included in this analysis. An organization's issues, if not stated outright, were made evident by the topics of published papers, conferences, and other services provided. If an organization did not state cyber security as a goal or issue, its activities were examined, and if less than half of its mentioned activities were on the topic of cyber security, the organization was excluded.

In all, more than 20 organizations were included in our analysis. Having identified the organizations, the next step was to determine each organization's spending on the CSTI. Most spending data come from IRS filings. These filings, through the 990 form and its derivatives, are publicly available upon request and are maintained by third-party databases. The most recent available data for each organization was from 2010 or earlier years.[49] Because of the aggregated nature of the published expenses for each organization, it is impossible to determine how much of each organization's budget was dedicated to cyber security. Therefore, an all-or-nothing approach was taken, in which the organizations we included were assumed to have contributed their entire budgets to cyber security, while organizations with less than a significant focus on cyber security had their spending left out entirely. This method resulted in a spending overestimation for the included organizations and an underestimation for the excluded organizations.

5.2.1 Key Organizations

Table 5-3 lists significant CSTI-contributing organizations, their revenue, CSTI expenditures, and the corresponding year of data. It is important to note that the total revenue and estimated expenditure listed for each organization do not include government grants (these are captured as government expenditures). However, revenue may include other public-sector sources of funding such as government contracts. Because much of the available funding information was aggregate, it was difficult to isolate government-sourced funding. However, a majority of organizations listed membership dues and advertisement revenue as primary sources of revenue.

The eight highest-spending organizations each invest over a million dollars a year. The following organizations account for over 95% of our total industry consortia spending estimates:

- **ISACA** ($29.3 million in 2011) publishes research and other educational resources and organizes conferences. The organization provides education, tools, benchmarks, and standards related to the security, governance, and auditing of information technology and information assurance (Information Systems Audit and Control Alliance, n.d.).

[49] In some cases, organizations have no data for 2010. For these organizations, spending information for the most recent year was used. In one case, spending information was estimated from data on the organization's website.

Table 5-3. Spending by Industry Associations and Consortia on the CSTI (2012)

Organization	Year	Total Revenue ($)[a]	Estimated CSTI Expenditures ($)[a]	Estimated CSTI Expenditures ($2012)[b]
ISACA[c]	2011	45,877,285	29,321,664	29,815,053
Internet Society	2010	26,044,866	22,525,676	23,627,704
Financial Services ISAC	2010	3,159,513	3,045,593	3,194,593
National Cyber Forensics and Training Alliance	2009	1,911,746	1,761,767	1,878,270
Center for Internet Security, Inc.	2009	1,466,191	1,401,306	1,493,972
WaterISAC	2010	1,779,269	1,296,832	1,360,277
Information Systems Security Association	2009	1,330,680	1,277,271	1,361,735
Forum of Incident Response and Security Teams	2010	1,283,925	1,157,232	1,213,848
Information Technology ISAC	2010	480,278	433,256	454,452
Information Card Foundation	2010	330,250	319,109	334,721
National Cyber Security Alliance	2009	319,257	298,215	317,935
Center for Applied Identity Management Research	2010	225,000	225,749	236,793
Federation for Identity and Cross-Credentialing Systems	2010	228,671	221,066	231,881
Online Trust Alliance	2009	226,673	181,641	193,652
Industry Consortium for Advancement of Security on the Internet	2010	150,234	150,238	157,588
Cloud Security Alliance	2009	76,089	139,416	148,635
Information Security Summit	2010	133,394	133,089	139,600
Colloquium for Information Systems Security Education	2010	329,246	126,434	132,620
Kantara Initiative	2011	N/A	95,000	96,599
United States Cyber Consequences Unit	2009	80,000	40,395	43,066
Energy Sector Security Consortium Inc.	2010	40,327	39,620	41,559
Total		**85,472,894**	**64,190,569**	**66,474,555**

[a] Figures in each cell in columns 3 and 4 have as their base year the year listed in column 2.

[b] Inflation data extracted from Bureau of Labor Statistics (2012a).

[c] Spending information comes from the ISACA (2012) Annual Report.

Note: Sums may not add to totals due to independent rounding.

Source: Guidestar, n.d.

- **Internet Society** ($22.5 million in 2010) develops standards, protocols, and Internet infrastructure technology; organizes events and conferences; and promotes policies that support the transparency and security of the Internet. The organization deals with many Internet-related issues, one of which is security. The Internet Society supports the IETF, an organization tasked with developing the Internet infrastructure, which contains several Internet security working groups. The Internet Society, in one of its several roles, "acts as a global clearinghouse for Internet security information and education" (Internet Society, n.d.) by developing original research and standards and sponsoring events and conferences like the annual Network and Distributed System Security Symposium.
- **Financial Services Information Sharing and Analysis Center (Financial Services ISAC)** ($3 million in 2010) provides information regarding cyber and physical security threats. The organization collects information on threats against financial service providers, analyzes the threats, and disseminates critical information necessary to protect against potential attacks (Financial Services Information Sharing and Analysis Center, 2011). The Financial Services ISAC is also involved in creating new technologies provided as a service to members. Recently, the organization developed a Critical Infrastructure Notification System allowing alerts to be sent to multiple member organizations almost instantaneously.
- **National Cyber Forensics and Training Alliance (NCFTA)** ($1.8 million in 2009) is a public-private partnership that is tasked with combating illegal electronic activity. The objectives of the alliance are to identify, mitigate, and neutralize cyber crime threats and to rapidly build intelligence to the actionable level so the threats can be identified, mitigated, and neutralized (National Cyber-Forensics & Training Alliance, n.d.). The NCFTA develops infratechnology by facilitating information sharing between subject matter experts and law enforcement and publishing reports regarding cyber threats. The actions of the organization lead to criminal and civil investigations and a higher level of preparedness against cyber attacks.
- **Center for Internet Security (CIS)** ($1.4 million in 2009) enhances public and private cyber security readiness and response. The organization has three major objectives, all of which develop infratechnology. The first objective is the development of benchmarks "that establish standards for the secure configuration of information technology systems" (Center for Internet Security, n.d.). The second is to provide services for monitoring, identifying, warning about, responding to, and mitigating threats and vulnerabilities at all levels of government. The third is to educate and train a cyber security workforce. Moreover, in alignment with its objectives, CIS publishes tools, metrics, white papers, newsletters, guides, other educational services, and a list of software certified by the organization.
- **Water Information Sharing and Analysis Center (WaterISAC)** ($1.3 million in 2010) is dedicated to the security of the nation's water resources with respect to the environment and public health. The organization collects and reviews intelligence from public- and private-sector sources so that member organizations can "identify risks, prepare for emergencies, and secure the nation's critical water infrastructure" (Water Information Sharing and Analysis Center, n.d.). By providing tools, best

practices, and 24-hour tracking services that furnish the critical information necessary to protect the water infrastructure, the WaterISAC provides infratechnology.

- **ISSA** ($1.3 million in 2009) educates managers and security professionals about cyber security best practices. The organization funds infratechnology by providing information through networking events, newsletters, and an official journal, with the ultimate goal of “promoting management practices that will ensure the confidentiality, integrity, and availability of information resources”(Information Systems Security Association, n.d.).
- **Forum of Incident Response and Security Teams (FIRST) (**$1.2 million in 2010) for educating and equipping incident response teams with resources and information to promote incident prevention and mitigation (Forum of Incident Response and Security Teams, n.d.). The organization contributes to infratechnology by developing tools and best practices for its members. Furthermore, it provides members with a forum to collaborate and create their own tools and best practices.

5.3 Spending by Private-Sector Firms

A third source of investment is carried out by private-sector firms. Firms invest in cyber security technologies in the following ways:

- proprietary technology for internal use,
- direct funding of industry-wide projects, and
- participation in industry associations.

Firms may invest in their own technologies or solutions. Interviews from our case studies show that very large firms may invest in proprietary, internal solutions to improve their own cyber security capabilities. Although such investments can be classified as CSTI, they often result in inefficient activities. For example, a private Firm A can develop its own internal proprietary cyber security technologies—e.g., a methodology for testing the level of security of a partner’s network or a set of best practices. Firm A, however, may have difficulty convincing a partner organization, Firm B, to trust Firm A’s security analysis of Firm B’s network or use its best-practice methodologies.

Direct funding (e.g., membership dues, grants, fees) by for-profit firms is generally included in the revenue estimates of the industry associations. Thus, the spending estimates of the nonprofit associations listed in the previous sections include financial contributions from for-profit firms. This section includes only the labor contributions of private firms when participating in consortia as well as internal investments.

In the IT security manager survey, discussed later in the report, respondents were asked if they participated in local, regional, or national consortia in 2010. Those that answered positively were asked to provide the number of person-hours contributed to industry consortia in that year. Among U.S.-based respondents, 130 respondents answered the question, listing an estimated total of 23,919 person-hours spent working with industry consortia. Responses ranged from 8,500 person-hours to 0 person-hours.

To extrapolate to industry-wide numbers, the total person-hours spent working with consortia was divided by the total employment hours of the respondents that provided numbers of person-hours (2,432,012). The resulting number was an estimated average of 0.0098 person-hours contributed to consortia per employee. Given the relatively small number of organizations providing this data for each industry, this overall average was used to calculate the estimated level of labor contribution for each industry. This number, 0.0098 person-hours, was multiplied by the 2012 employment estimates for each industry, and that number was further multiplied by each industry's IT intensity multiplier.

The IT intensity multiplier represents the degree to which, for each industry, the average IT spending as a percentage of revenue varies from the national average. The ratio of x_i/y is used, in which x_i is the IT spending (as a percentage of revenue) for each industry, and y is the national IT spending as a percentage of revenue. For instance, if the national average is 6%, and industry A has an IT budget of 3% of revenue, the industry's multiplier would be 3/6 = 0.5. The result of the multiplication can be seen in Table 5-4.

The final step was to estimate the dollar value of this labor contribution. An average wage for a cyber security professional was estimated by averaging the mean hourly wages of the following occupations:

- Chief executive
- Computer and information systems manager
- Information security analyst, web developer, and computer network architect.

The wage categories and amounts were extracted from the Bureau of Labor Statistics (2012b), and wages were split by industry. The three particular wage categories above were chosen because of their representation of the range of survey respondents' job titles.[50]

To represent a total hourly cost per employee (accounting for nonmonetary benefits and overhead costs), we multiplied wages by 2. The resulting cost was multiplied by the extrapolated number of person-hours spent in consortia, and Table 5-4 displays the results. Approximately $146.8 million was spent by private firms in 2011 in collaboration with industry consortia.

[50] Note that the "chief executive" category was included because a significant number of people who responded to our survey listed their role as chief executive officer or chief security officer; the salaries of both are included in this category.

Table 5-4. Estimated For-Profit Labor Spending on Industry Association and Consortia Activities, by Industry (2012)

Industry	Person-Hours Spent in Consortia per Employee	Total Industry Employment	IT Intensity Multiplier	Person-Hours Spent In Consortia (Extrapolated)	Estimated Hourly Cost Per FTE[a]	Estimated Total Labor Spending In Consortia
Mining, quarrying, and oil and gas extraction	0.0098	651,631	0.47	3,015	$130	$392,545
Utilities	0.0098	551,287	0.98	5,314	$127	$675,385
Construction	0.0098	5,489,499	0.47	25,400	$116	$2,968,429
Manufacturing	0.0098	11,487,496	0.89	100,103	$130	$13,050,122
Wholesale trade	0.0098	5,466,463	0.55	29,508	$129	$3,835,850
Retail trade	0.0098	14,481,324	0.55	78,171	$119	$9,348,523
Transportation and warehousing	0.0098	3,943,659	1.22	47,138	$118	$5,595,889
Information	0.0098	2,703,886	1.90	50,564	$140	$7,096,498
Finance and insurance	0.0098	5,486,241	1.78	96,249	$139	$13,400,355
Real estate and rental and leasing	0.0098	1,915,571	1.76	33,237	$125	$4,160,922
Professional, scientific, and technical services	0.0098	7,457,913	1.76	129,402	$136	$17,701,187
Management of companies and enterprises	0.0098	1,854,778	1.76	32,182	$138	$4,458,243
Administrative and support and waste management and remediation services	0.0098	7,399,320	1.76	128,385	$119	$15,348,839
Educational services	0.0098	2,460,150	1.84	44,583	$104	$4,648,566
Health care and social assistance	0.0098	16,196,009	1.25	199,834	$113	$22,678,453
Arts, entertainment, and recreation	0.0098	1,903,739	1.76	33,032	$119	$3,937,182
Accommodation and food services	0.0098	11,103,075	0.47	51,373	$97	$5,002,365
Other services (except public administration)	0.0098	4,349,563	1.76	75,469	$110	$8,369,441
Total		**104,901,604**		**1,162,961**		**$142,668,803**

[a] Estimated hourly cost per FTE is double the BLS-provided hourly wage

Source: RTI data and Bureau of Labor Statistics Occupational Employment Statistics (2012b) and Current Employment Statistics (2012c). Shaded rows are used to highlight the key industries included in the case studies during this project.

Note: Sums may not add to totals due to independent rounding.

5.4 CSTI Investment Summary

Table 5-5 summarizes the estimated public- and private-sector investments in the CSTI in 2012. The public sector is the biggest spender, contributing just over 70% of total investment to the CSTI. The combined effort of the private sector has contributed about 30% of total spending. Yet spending for the private sector may be underestimated, because it is likely there are several organizations activities were not captured in this analysis. Having inferred a baseline estimate of cross-industry and public-sector spending, the next step is to gain insight from private firms on the costs and benefits of potential advancements in the CSTI.

Table 5-5. Summary of Public- and Private-Sector Investment in the CSTI (2012)

Type of Organization	Estimated CSTI Spending ($ million)	Percentage of Total Spending
Federal government	506.9	70.8
Nonprofit industry consortia [a]	66.5	9.3
For-profit corporations [a]	142.7	19.9
Total	**716.1**	

[a] These estimates were adjusted to 2012$ based on data from the Bureau of Labor Statistics (2012a).

Note: Sums may not add to totals due to independent rounding.

6. GAPS IN THE CYBER SECURITY TECHNICAL INFRASTRUCTURE

As described in Section 3, case-study style interviews with 36 organizations' cyber security directorates solicited information on key CSTI gaps that, if narrowed by 10%, would have significant beneficial impacts on their cyber security operations. These interviews were complemented by a series of expert elicitation interviews with 25 security experts to identify specific infratechnologies that, if developed, could narrow the gap in each of the CSTI areas by at least 10%. Table 6-1 provides an overview of the primary market failures underlying each of the nine CSTI gap areas.

In this section, we describe the CSTI areas and the gaps proffered by industry and then provide recommendations for CSTI investment that security experts believe would narrow those gaps. This information provides an explicit roadmap on which potential CSTI investments are expected to have the greatest economic impact on U.S. organizations. The following is reviewed for each CSTI gap:

- Characterization of the gap and data from our research and interviews,
- Discussion of the market failures affecting investment in each gap, and
- Discussion of interviewee recommendations and potential solutions for narrowing the gap.

6.1 Inadequate Authentication of All System Users

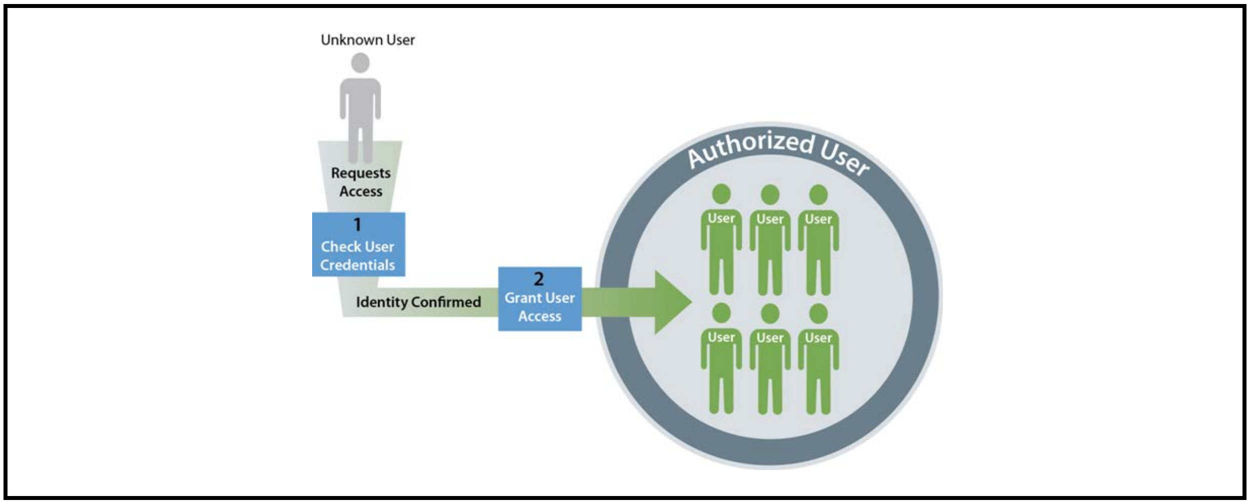
Authentication is the process by which an organization's users—employees, vendors, contractors, or customers—have their identities verified through the use of a credential or set of credentials each time they request access to protected data or resources (Figure 6-1). Currently, most companies' internal and external authentication strategies are based on simple user name and password combinations; however, this is an inadequate method of authentication because of weak passwords and the increasing ability to steal or identify passwords. More advanced authentication strategies, including multifactor authentication and federated identification, are emerging, but the infrastructure that would enable widespread adoption is currently insufficient.

Multifactor authentication can help improve the security of IT systems by requiring the use of a combination of factors—such as a username and password, personal identification number (PIN), personal verification questions, biometrics, possession of a hardware device (e.g., a smart card, USB device, or smartphone) or software application, and user behavior—before access is granted. Authentication systems based solely or primarily on user names and passwords

Table 6-1. Primary Market Failures Motivating Government Role, by CSTI Gap Area

	Nature of the Market Failure			
CSTI Gap Area	**Public Goods**	**Network Effects/ Externalities**	**Coordination Failure**	**Uncertainty / Imperfect Information**
Authentication of all system users		●	●	●
Sharing of or access to threat data	●		●	
Specification and collection of security metrics	●		●	●
Mobile device security		●		●
Cloud security		●	●	●
Automated threat detection and prevention		●	●	●
Protection and mitigation from loss of equipment and media			●	
Education about IT security best practices and threat awareness		●		●
Standards for meeting auditing and compliance requirements			●	●

Figure 6-1. User Authentication



Source: RTI International.

are very susceptible to compromise.[51] Currently, multifactor authentication is being used by some organizations[52]; however, this technology is far from being universal, and there has been little detectable effort to provide clear standardized guidelines or means of measuring effectiveness. In addition, evaluation of solutions is important, because not all technologies are perfect. An example is the breach of RSA's SecurID tokens mentioned in Section 2.4. [53]

Federated authentication, for the purposes of this discussion, is defined as a framework in which a single set of credentials (single or multifactor) can be used to gain access multiple systems. Also known as third-party authentication, with federated authentication, identity providers such as banks and credit agencies would verify individuals' identities and provide them with credentials. Individuals could use the same credentials to access their online banking, health care provider's website, and their tax return. Widespread adoption of a federated authentication system would relieve users of the difficulty and risks of maintaining multiple identities with different providers and systems, and it would relieve service providers of onboarding and maintaining registration information.

To achieve a system based on federated authentication, a variety of standards, protocols, and standard operating procedures are needed. Adoption of existing standards supporting federated authentication, however, has been slow. The field is fragmented, with no one prevailing standard.[54] The White House's National Strategy for Trusted Identities in Cyberspace, or NSTIC (2011), aims to promote widespread adoption of federated authentication by creating an identity ecosystem in which independent entities can verify the identities of individuals and organizations accessing services online. Together, NIST and NSTIC's National Program Office is coordinating the development of new standards, policies, and procedures to increase the use of federated authentication.[55] In order for federated authentication to be viable, infrastructure must be in place that allows identity providers and parties that accept credentials that relying parties issue to individuals to communicate securely and with a high level of assurance that those credentials have not been compromised in some way.

[51] For example, the Utah Department of Health recently suffered from a data breach in which 280,000 individuals had their social security numbers stolen; the cause of the attack was a hacker exploiting a weak password on the system (Horowitz, 2012).

[52] For instance, some banks may send a customer a code via e-mail, phone call, or text message to access a bank's website from a particular computer.

[53] A 2011 attack on RSA's SecurID tokens, devices that generated a single-use password, led to a leak of the algorithm used to generate the temporary passwords. This leak led to further attacks against several high-profile defense contractors, in which attackers were able to pass the victim organizations' authentication controls (Whitney, 2011).

[54] Examples of such standards include OpenID, Security Assertion Markup Language (SAMUL), and Shibboleth.

[55] An ongoing NIST study, to be published in January 2013, involves a case study analysis of the net benefits of NSTIC adoption by the Internal Revenue Service (IRS).

6.1.1 Support from Interviews with Industry and Security Experts

Companies we interviewed generally used only username/password credentials for authentication, which some judged as inefficient and unsustainable. Moving forward, authentication is likely to become even more important to them as new technologies increase the number of ways in which employees, partners, and customers want to connect to company networks. As a result, organizations in the health care industry were particularly concerned about the growing connectivity of systems containing electronic medical records and managing access for a growing number of doctors across several organizations and geographic areas.

Security experts all noted that industry widely acknowledges the inadequacy of their authentication models, but adoption of more advanced technologies remains slow. As such, there is a significant role for the government to play to help create an environment in which improved authentication technologies would thrive, for example through new infratechnologies to support comparative assessments of competing technologies.

Of note, several companies specifically mentioned the 2011 compromise of RSA’s SecurID tokens as a warning that non-password controls are not entirely infallible. This suggests that new generic technology may be needed—e.g., new models for authentication beyond those currently envisioned.

6.1.2 Market Failures Preventing Improved Authentication of All System Users

Several market failures have prevented the development of the necessary CSTI to support improved authentication options. *Imperfect information* about the total cost of inadequate authentication and *information asymmetries* in which providers of multifactor authentication solutions know more about the level of security that their products provide than organizations (potential customers) know negatively affect the market for improved authentication. Because of these market failures, organizations are unable to make investment decisions based on a full understanding of the costs and benefits of different authentication solutions or compare competing solutions.

Further, a *coordination market failure* impedes widespread adoption of federated authentication as adoption costs for enhanced authentication are significantly lower with coordinated adoption than go-it-alone approaches. Coordination problems further inhibit the ability of private organizations to work together to develop the necessary standards and other CSTI. The *network effects* and the *chicken-and-egg nature* of federated authentication means that organizations benefit from widespread adoption (lower costs); both identity providers and relying parties do not want to invest in infrastructure, so both groups are waiting for the other to move first.

6.1.3 Recommended Improvements in the CSTI

The current inadequacies of authentication could be improved by new CSTI to increase adoption of federated authentication and multifactor authentication. In addition to improving current costs, these authentication frameworks are especially important in dealing with the growth of online services and cross-platform authentication.

A possible solution to the slow pace of adoption could be a thorough assessment of the technology choices, perhaps in the form of an open competition,[56] as suggested by one security expert. This would help develop consensus on which technologies work, which do not, and which should ultimately be adopted. Information to aid with making comparisons could also be increased through the development of standards or standard test methods that organizations could use to objectively compare authentication technologies and ensure compliance with desired performance specifications.

A broad approach to standardizing technology ratings, performance classification, definitions, and mapping would be valuable to those providing and relying on authentication services and to policy makers who are responsible for protecting the public. Vendors have proprietary approaches and products and do not seem inclined to voluntarily develop new guidelines and evaluation methodologies. As such, NIST could contribute by developing a strength rating scheme that, in a coarse way, would allow users and providers to discern how well a particular choice would protect them.

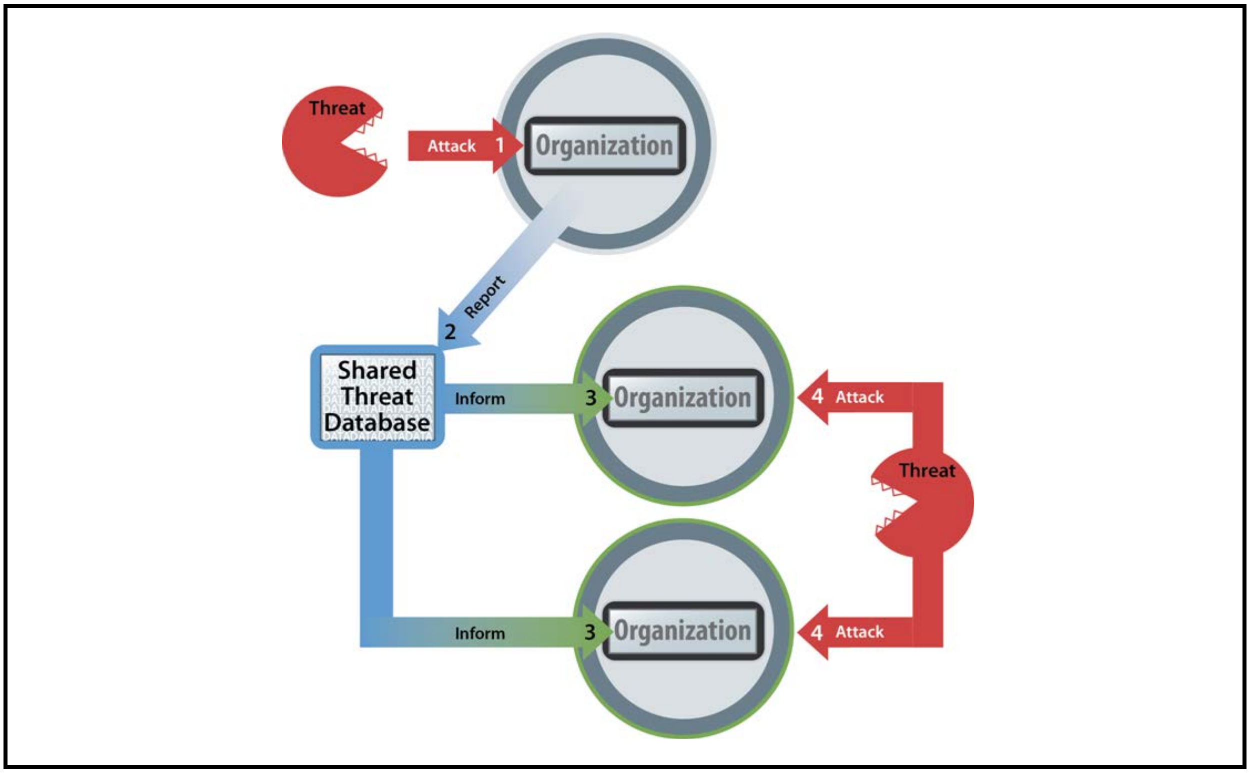
Currently, the NSTIC National Program Office at NIST is working with public and private sector stakeholders to develop consensus standards and standard policies and procedures. For example, federal government agencies seeking to accept third party credentials are only allowed to accept credentials from GSA-approved identity providers based on a set of guidelines established by NIST, and the private sector can also leverage such approval information to make decisions. Additional standards and other infratechnologies need to underpin any such authentication system in order to motivate adoption by organizational stakeholders and individuals; however providing adequate (i.e., clear and concise) information for individuals offers a separate challenge.

6.2 Inadequate Sharing of or Access to Threat Data

Sharing information on threats helps companies stay protected from potential attacks they are unaware of (Figure 6-2). Shared threat data refers to information about cyber attacks that victims share with other companies or with a single organization set up to collect threat data.

[56] Such a competition could include prizes or simply credibility/reputational benefits to the winner. The later "prize" is the benefit that accrues to winners of the annual NIST Text REtrival Conference (TREC) competitions, through which information retrieval systems are evaluated annually. See information at http://trec.nist.gov.

Figure 6-2. Shared Threat Data



Note: The figure sequentially shows an initial attack getting through an organization’s defenses. Once that organization recovers and reports information about the attack, a group maintaining a threat database can share this information with other organizations, which are able to repel attacks of a similar nature.

Source: RTI International.

Any identifiable information about a source of an attack or method of attack is valuable when used in aggregate or when similar attacks occur. Collecting and analyzing threat data can reveal trends to inform counter measures.[57] Sharing threat data can improve efficiency. For example, if a cyber criminal attacks multiple companies, one after the other, the companies already attacked may have information that can prevent subsequent successful attacks of the same nature directed at other targets. Many kinds of attacks can be successfully thwarted or mitigated if sufficient threat data are available.

Broadly, the sharing of threat data is already carried out by several public and nonprofit organizations. US-CERT is the federal government’s primary means of coordinating cyber security.[58] The US-CERT portal provides a “secure, web-based, collaborative system to share sensitive, cyber-related information and news with participants in the public and private sector”

[57] For example, antivirus software companies operate as information sharing organizations. Every time a virus is caught, data are collected to find virus trends and to develop software updates for all users.

[58] US-CERT was developed to implement the National Strategy to Secure Cyberspace (NSSC), established to prevent, reduce vulnerability to, and minimize damage from cyber attacks in America.

(US-CERT, n.d.). US-CERT partners with a variety of organizations, including Information Sharing and Analysis Centers (ISACs).[59] NIST also provides data on threats through its management of the National Vulnerability Database (NVD), and DHS is developing pilots with financial firms and state governments to collect and share classified threat data with select individuals at partner organizations (Miller, 2010).

However, government agencies are generally reluctant to release classified data, and companies are also reluctant to share data because of "fear of losing control over personal or proprietary information" (Nakashima, 2009). These concerns are preventing the establishment of more prevalent information exchange.

6.2.1 Support from Interviews with Industry and Security Experts

Several companies interviewed during case studies mentioned their concern that any data they share may be traced back to them. One company said that they were "… primarily concerned about exposing their vulnerabilities to competitors and would-be attackers."

However, companies are sharing some data. Several interviewees mentioned that, typically, they find out about attacks against other organizations informally, usually through outside contacts. One interviewee mentioned that security professionals are generally more likely to exchange information using personal connections rather than official databases. This data sharing provides benefits to those who participate, but many companies are not included. Further, the number of companies involved in such informal information sharing is limited, so data is not shared among a larger group through such mechanisms. Thus, a complete and aggregated threat picture is not available through informal networks.

Experts also noted that information sharing currently occurs regularly through a variety of private sector relationships including through companies' relationships with consulting firms (e.g., Deloitte), research firms (e.g., Gartner and Frost & Sullivan), and security service providers (e.g., AT&T, IBM, Verizon, and Symantec). Companies discuss threats and vulnerabilities with these firms and the firms use all such information to provide advice to other customers (companies).

6.2.2 Market Failures Preventing Improved Sharing of or Access to Threat Data

Currently there is no commonly agreed upon format by which threat data is captured and reported within organizations, and there is no standard format in which partially or fully anonymous threat data can be shared among organizations. No single company will invest

[59] According to the National Council of ISACs, many ISACs have strong penetration in their respective industries, and all ISACs provide services such as "risk mitigation, incident response, alert and information sharing" (National Council of ISACs, n.d.).

sufficiently in the development of such standards because of the public-good nature of shared data.

Further, a company may be concerned that it would ultimately harm itself by sharing information on threats and vulnerabilities. Information regarding a company's defenses and vulnerabilities could be used to embarrass the company, bring unwanted attention, or potentially cause damage to revenue or reputation. If all companies shared threat and vulnerability data, then all companies would incur these risks; as such, the failure to do so can be considered a coordination market failure. Without coordinated action, no company is motivated to share information and put themselves at a competitive disadvantage.

6.2.3 Recommended Improvements in the CSTI

Organizations, including federal agencies, recognize that sharing attack data would benefit their preparedness; however, many barriers exist that prevent them from using existing tools and standards to share cyber attack data. These include the gathering of data, specification of formats or exchange protocols, legal and other formal agreements to protect anonymity, and private incentives. To solve this issue, there must be effective and reliable ways of ascertaining that the data submitted by a company is made anonymous. Making the data anonymous would require contributors to specify the level of data anonymity, aggregation, or generalization they require to address their concerns about sharing the data. Moreover, the organization collecting, managing, and distributing the threat data must be trusted to adhere to any specification of anonymity.

Information that could be made anonymous includes the identity of the contributor, details of network and defensive system configurations, and specifics of the damage caused by breaches. Despite past work, more may need to be done to find ways to make data sufficiently anonymous while retaining its usefulness.

The public sector should seek to develop a consensus on the incentives that should be used / manipulated and the implementation strategy for manipulating incentives. Possible incentives include subsidies, contribution requirements before benefiting from shared data, recognition, mandates through legislation, or the establishment of a marketplace for shared data.

6.3 Inadequate Specification and Collection of Security Metrics

Companies may also be ineffective at stopping or preparing for attacks because they do not adopt and collect data against proper security metrics about their risk profile. Metrics represent an analysis of a set of measurements and an interpretation of the same. Security metrics can be used to measure the effectiveness of particular tools or policies. Moreover, they can enable insight into a company's cyber security landscape to help identify particular threats and vulnerabilities. Most important, metrics can show where a company should be focusing its efforts to correct a misunderstanding of risk.

Collecting the right security metrics and deriving meaning from them is challenging. For example, the number of security incidents and breaches a company experiences could be used as one estimate of a company's level of security; however, definitions of the terms incidents and breaches differ across organizations. Further, correlating the number of security incidents and breaches with specific security policies or measures, to ascertain the impact of a given security tool or policy, would be precluded by an absence of appropriate characterization of incidents and breaches.

6.3.1 Support from Interviews with Industry and Security Experts

Efforts have been made to develop security assessment standards and metrics in the past;[60] however, each such attempt has "obtained only limited success" (Jansen, 2009). Security experts interviewed indicated that this occurred because of a lack of broad agreement on a high-level set of security objectives. Individual security managers differ widely in their opinions of what security objectives are most important; this heterogeneity in opinions is based on a variety of factors including security managers' training and experience, and the culture of the company and its industry, among other factors.

It appears to be far more common for security managers to measure data qualitatively than quantitatively. This means that assessments of information security performance and effectiveness are not typically based on objective interpretation of standardized data but are rather based on the observation and intuition of the evaluator. Because of the subjective nature of such security assessments, they are often not repeatable or measurable in a commonly agreed-upon way. As can be seen in the world of public health, metrics help to enable organizations to track their performance internally as well as to compare against other organizations such the same metrics.[61]

Further, several companies noted the need for technical security metrics to be translated into business value/impact. According to a Director of IT Security at a large retail company, "without adequate security metrics, I currently try to use fear to convince our CEO into investing in security by pointing to regulations that may impact us if we're not secure enough and identifying stories in the media about the potential fall out of breaches."

[60] Several examples include: Trusted Computer System Evaluation Criteria (U.S. Department of Defense), Information Technology Security Evaluation Criteria (researchers in several European countries), Systems Security Engineering Capability Maturity Model (International Systems Security Engineering Association), and Common Criteria (International Standards Organization).

[61] It is important to note, however, that as the public health community has shown, continual updating of metrics and evaluation methodologies is also critical to ensure the metric collected and evaluations conducted are based on the best information available. The same continuous improvement model is needed to maintain effective cyber security metrics and evaluation methodologies.

Our interviews also gave insight into the need to improve the collection of metrics themselves. Some companies need to efficiently aggregate and query data that are distributed across systems and locations, and they often are not able to get a centralized view of the threat profile across all business units. Good metrics require good methods for data collection.

Finally, several experts suggested that security metrics are the most important CSTI need that exists. Improving security metrics, they noted, could have a dramatic impact on the ability of security managers to make more cost-effective investment decisions based on objective analyses and then retrospectively analyze the results of their investments to discern the outcome.

6.3.2 Market Failures Preventing Improved Specification and Collection of Security Metrics

Broadly, the current lack of security metrics causes companies to make inefficient cyber security investment decisions based on an imperfect information market failure. Market failures also affect the level of investment in developing security metrics (a CSTI investment). Security metrics have a public-good component so one company cannot accrue the full value from CSTI investments in the development of security metrics without giving value to other organizations. The primary value in security metrics, as in other types of standards, comes from use by multiple stakeholders, a result of network effects. This reduces an individual organization's incentive to invest in developing security metrics. A coordination failure also exists as many firms need to work together to identify a set of metrics that could be useful and collected cost effectively.

6.3.3 Recommended Improvements in the CSTI

Robust security standards for measuring how much security is "good enough," standards for certifying security, and practical tools for measuring security are all greatly needed. At a basic level, common definitions describing well-understood functions are needed, after which useful metrics can be identified and standards and tools developed. Without these, organizations find it difficult to justify potential investments, to compare the choices and intelligently select the best ones, or to tell if actual investments are achieving their intended goals.

NIST could provide a valuable contribution to the CSTI by developing and standardizing a set of security metrics and measurement tools. Potential research areas suggested by experts at NIST and elsewhere include the development and assessment of new formal security models, analysis of historical data to help identify key metrics, and investigation of artificial intelligence techniques for measuring security metrics.

The most lasting contribution would be to define a framework or methodology by which metrics could be developed and standardized, based on a consensus approach to ensure that organizations widely agree on their approach. Our interviews suggest that private organizations would welcome a well-reasoned approach to defining metrics. Such a framework would enable interested communities to debate and agree on the metrics that are most suitable for their needs, in accordance with principles and a process recommended by NIST. And private organizations will benefit from government expertise in measuring attacks, allowing them to better use their own existing resources for cyber security.

Additionally, some security experts pointed to "big data" analysis as an area of research that could benefit objective analysis of security. Because it is easier to collect large volumes of data today than it was in years past, companies have the potential to derive a more comprehensive and wider variety of information by aggregating and querying large amounts of data.[62] For example, companies can collect and store data on staff computing behavior and location and use such data to help anticipate potential attacks, either by insiders or through staff devices being operated in high risk areas (e.g., via a mobile phone in a coffee shop in New York). However, of note, the data of a single enterprise are distributed across locations, often resulting in a latency barrier to collecting and querying data rapidly in a central location. Standards could be developed to optimize the format of data transmitted within an enterprise or across multiple enterprises.

6.4 Inadequate Mobile Device Security

Mobile devices such as smart phones, tablets, and wireless scanners are being used to increase productivity by allowing employees to access data and applications from beyond the office, roaming on myriad networks domestically and internationally. These mobile devices are at great risk of being attacked remotely as a result of the insufficient level of security built in to many mobile devices and their software. Current technologies supporting mobile device security are inadequate as a result, primarily, of an information gap.

The security risks present in mobile devices such as smart phones are made worse because of their dual use as personal and work-related devices; they travel with the user to different environments with varying levels of security. Inevitably, some of these devices will be misplaced or stolen, which often leads to substantial data losses or leaks. Further, risky behavior of employees poses a primary threat to an organization's intellectual property and internal policies.[63] The strongest security measures cannot prevent employees from accidentally breaking policy and exposing an organization to unnecessary risk.

A common way to intercept mobile data is through a "man-in-the-middle" attack, in which a third party (a malicious actor) accesses, modifies, or inserts new data into the link between a mobile device and the host to which it is connected. Another way to compromise

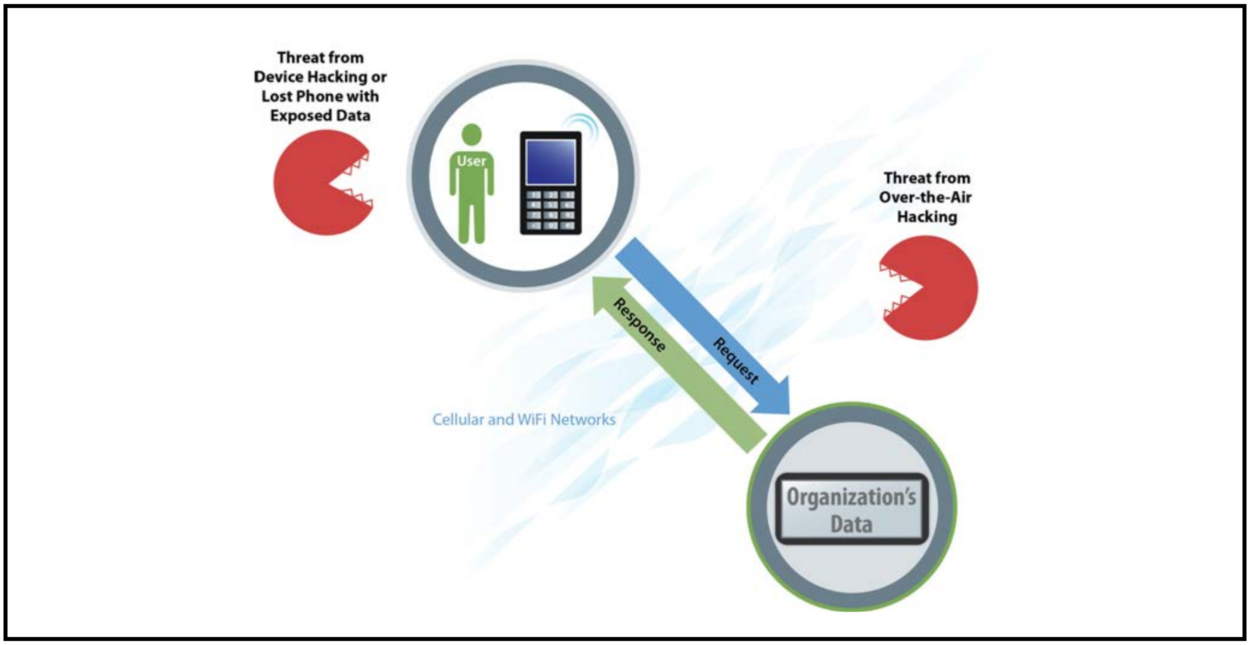
[62] Our interviews suggest a consensus among security experts that a simple algorithm for identifying threats based on a large sample would be more accurate than a more complex algorithm based on a small data sample.

[63] Further, employees may engage in risky behavior, such as using weak passwords, not securing mobile devices, navigating to illegitimate websites, or inappropriately using social networks, which increases the likelihood of accidental data loss and susceptibility to outside attacks.

mobile data is through theft or loss of a mobile device itself. Often, the only measure of security preventing a potential thief from accessing sensitive data is the device's unlocking password, assuming it is even active. The methods of attack are demonstrated in Figure 6-3.

There are standards for ensuring wireless encryption and password protection of wireless networks[64]; however, existing security solutions do not satisfy the needs of the wide range of mobile devices in use by the workforce. Most such solutions focus on protecting a single platform of devices, such as iPhones, BlackBerries, or Android devices; however, solutions that protect multiple platforms within a single enterprise are lacking. Security solutions available on BlackBerry devices may be unavailable or underdeveloped on iPhone or Android devices. Moreover, the technology and usage of mobile devices are still rapidly evolving. NIST has provided a variety of guidance recommendations for mobile security,[65] including *NIST SP 800-124 Revision 1 (Draft), Guidelines for Managing and Securing Mobile Devices in the Enterprise* (2012b). but interviews suggest that more work in this area is needed.

Figure 6-3. Mobile Device Threats


Threat from Device Hacking or Lost Phone with Exposed Data
User
Threat from Over-the-Air Hacking
Response
Request
Cellular and WiFi Networks
Organization's Data

Source: RTI International.

[64] The Institute of Electrical and Electronics Engineers (IEEE) has developed wireless encryption and password protection standards for wireless networks (SANS Institute, 2005). Device-specific solutions also exist, such as the BlackBerry Enterprise Solution, which many federal organizations use as a messaging platform (Booz Allen Hamilton, 2009).

[65] See an overview of all of NIST's work on mobile security at http://csrc.nist.gov/documents/nist-mobile-security-report.pdf.

6.4.1 Support from Interviews with Industry and Security Experts

Our interviews suggest that companies often assume that desktop and mobile devices have similar risk profiles, when, in reality, mobile security solutions are less available and less effective than those for desktop systems. This gap may be explained by a lack of risk assessment frameworks for mobile devices.

Security experts perceive mobile device security as a significant gap, the extent of which companies are only recently beginning to become aware. Experts suggest that based on the current technology trajectory, adoption of security technologies will increase only gradually until several public breaches make investment more easily justified.

6.4.2 Market Failures Preventing Improved Mobile Device Security

The gaps in mobile device security are caused by the growing number and complexity of mobile technologies and a company's inability to manage these various devices. The misperception of mobile security further contributes to this gap. All of these issues relate to issues of imperfect information—mobile security companies have not come up with a way to sufficiently communicate the comparative quality of their products— and information asymmetry—often they know more than the companies buying such products.

6.4.3 Recommended Improvements in the CSTI

Several security experts recommended the development of a standard to help characterize the security capabilities of smart phones, culminating in the assignment of specific security level/rating. These reference levels could bring significant clarity to the marketing and configuration of these devices and could improve users' understanding of mobile security. As with the NIST recommendations, this would decrease the uncertainty and asymmetrical knowledge issues that result in companies adopting either the wrong security features or no features at all.

Another role for NIST could be in the development of privacy standards for device tracking. Organizations want to be able to monitor device location for security, but this capability is eyed suspiciously by users. Recent events have demonstrated that neither the smart phone vendors nor the carriers are likely to protect these data in the way that a company or its users would be willing to accept. A clear-cut description of the choices that a company can make with respect to location information and how it can be used could serve as the basis for informed consent by device owners and for the development of market-based mechanisms (e.g., trusted brokers) for acceptable device tracking and localization.

The desire by users to transfer sensitive information to mobile devices for convenient access is problematic, as by definition, such devices will be used outside the traditional perimeter of the organization. One security expert suggested that a model of security similar to digital rights management (DRM) for such information might be appropriate. This would provide highly flexible but also closely controlled use of and access to data, based on parameters such as identity, situation (time and location of use), cryptographic protection, type of access required, and application used.

6.5 Inadequate Cloud Security

Another growing risk is the increased usage of cloud-hosted data and applications. NIST defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (NIST, 2011b). Using cloud computing brings several benefits to a company.[66] Unfortunately, increased use of cloud computing is also putting companies at an increased risk of a cyber security attack, given the lack of widely accepted cyber security standards, policies, and procedures for cloud computer environments. Because data are being hosted by a third party, the security of the data is only as strong as the security offered by the provider (Figure 6-4).

Possibly the most significant barrier to greater use of cloud computing is organizations’ concern about losing control of their security environment—i.e., losing physical control of information assets and reducing the ability to easily identify access points. For companies that are impacted by various cyber security regulations, cloud computing is very problematic, as the ability to physically control data and to be able to identify the location of specific pieces of data is a critical component of compliance with many regulations.

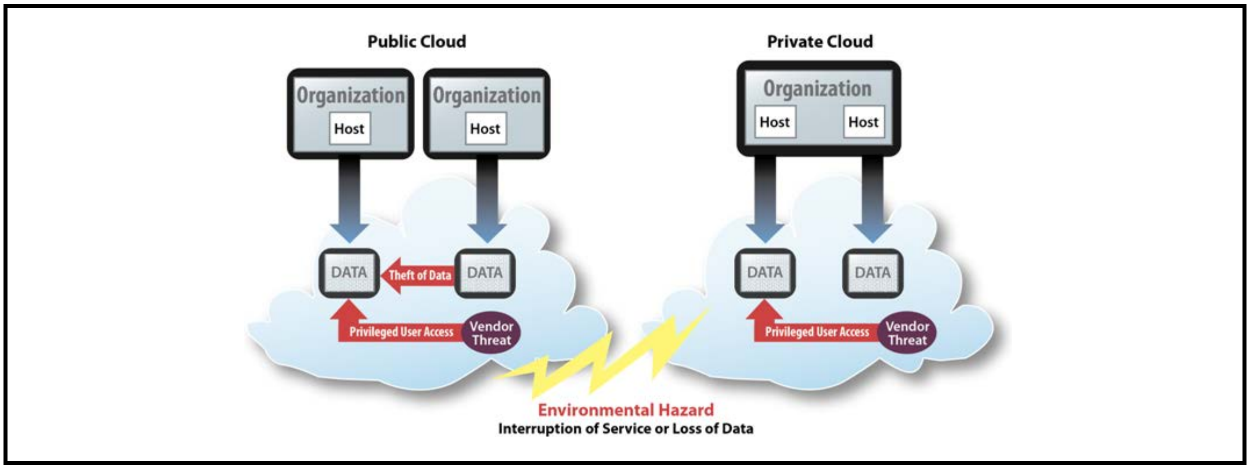
Several organizations have provided CSTI to support cloud computing. The Cloud Security Alliance (CSA) has developed and published a variety of tools, frameworks, protocols, and reports for all aspects of cloud security.[67] NIST has also provided substantive guidance on cloud computing security, including several recent recommendations and guidance publications.[68] Such materials could be used to support cloud-computing users and vendors negotiating the security characteristics of cloud computing services; however, at present, cloud vendors have not shown significant interest in providing security guarantees, transparency, or auditing.

[66] Cloud computing does not impose any direct capital expense. In addition, there are generally lower variable costs; due to economies of scale, companies pay less for maintenance and labor. Cloud solutions are also quickly deployable and scalable; adding space for applications is fast, and customers pay only for the traffic and hosting space they use.

[67] For example, the CSA’s GRC Stack provides a method to assess “both private and public clouds against industry established best practices, standards and critical compliance requirements” (Cloud Security Alliance, n.d.).

[68] NIST’s *Cloud Synopsis and Recommendations*, released in May 2001, provided a set of recommendations for cloud security. And in December 2011, NIST released *Guidelines on Security and Privacy in Public Cloud Computing* (NIST, 2011c), an extensive reference document for customers of cloud computing. This document identifies novel risks associated with cloud computing and has recommendations for potential users to consider.

Figure 6-4. Cloud Computing Threats



Source: RTI International.

6.5.1 *Support from Interviews with Industry and Security Experts*

Despite ongoing efforts to improve cloud security, significant security concerns remain, posing a large barrier to the adoption of cloud services. The 2010 Ernst & Young‘s Global Information Security Survey found that roughly a quarter of respondents used a cloud computing solution that year. The respondents using cloud computing outlined three important risks: data leakage (52%), loss of visibility of what happens to company data (39%), and unauthorized access (34%).

These concerns were confirmed by our interviews. One company mentioned that evaluating the security of multiple cloud service providers proved very difficult, costly, and time-consuming. Similar to mobile security, the quality of the security of cloud computing services is not well known or understood, and even further, it is very likely that cloud computing service providers know much more than their customers do about the security of their products and services.

Moreover, interviewees reported a number of issues preventing the adoption of cloud computing. One issue was that of liability; cloud subscribers need to understand the legal and contractual obligations of cloud providers before using their services. Subscribers need a way to understand all of a provider’s security offerings and evaluate its risk profile. These gaps are not yet addressed by existing standards. Moreover, interviewees mentioned that much of the output from the CSA does not apply to cloud computing subscribers.

6.5.2 *Market Failures Preventing Improved Cloud Security*

The gaps present in cloud computing security are due to several existing market failures. First is the disconnect in incentives (i.e., customers may not be willing to pay substantially more for security, and as such service providers operating with inefficient CSTI infrastructures and therefore higher costs scale back the amounts supplied). Further, information asymmetries exist in the market (i.e., usually cloud providers know more about the cloud and security issues than their customers). A relationship almost certainly exists between customers’ relative lack of information on the security of cloud services and their lack of expertise to interpret the security implications of specific cloud services (e.g., they are unable to monetize the risk appropriately). The consensus is that potential cloud customers do not have sufficient information to make an informed decision to choose the cloud provider that is the most secure fit for their needs.

6.5.3 Recommended Improvements in the CSTI

Providers of cloud computing services have been reluctant to include security as part of their service guarantee. If security capabilities are offered, often it is left to the customer to install, configure, and monitor them. This means that both scale and scope economies are not realized. In addition, there may be little recognition of the additional risks that cloud computing poses (e.g., multiple, possibly antagonistic, users sharing a computer, collocation of data on shared storage devices). Improvements to the CSTI could enable cloud computing services providers to increase security more efficiently and effectively and increase cloud computing customers’ confidence in the security of cloud computing, resulting in an increase demand for cloud computing services and reduced marginal cyber security costs.

According to security experts, two major difficulties need to be addressed. The first is the lack of adequate security metrics. The situation is exacerbated by the additional complexity of cloud computing (e.g., virtualization, dynamic provisioning, migration, collocation). Lacking clear metrics, a contract can focus only on processes, not on requirements or measurable results. A second difficulty is the premium cost imposed by security and privacy requirements. Cloud computing accelerates the trend of decreasing computation, storage, and bandwidth costs but, at the same time, increases the costs of administration and monitoring. The difference between those two factors can be several orders of magnitude (that is, infrastructure may cost hundreds of dollars per month, and technical support may cost thousands or tens of thousands of dollars a month). This difference emphasizes to an even greater degree the high cost of security, tempting users to forgo expensive services.

Investment by NIST in cloud computing security offers multiple benefits. Users will have more influence over the services offered to them and can negotiate more effectively to meet their needs. Clarity in the choices and possibilities of cloud solutions may encourage an even higher degree of interest in cloud computing. Cloud security infratechnologies will enable organizations to efficiently choose, from among the solutions available to them, the most optimal cloud solution. Finally, the gap between regulations and technical capabilities may encourage regulatory bodies to update their requirements in light of this new technology.

6.6 Inadequate Automated Threat Detection and Prevention

Primarily, organizations stop breaches by employing intrusion detection or prevention software. NIST defines intrusion detection and prevention systems (IDPSs) as “software that helps organizations to monitor and analyze events occurring in their information systems and networks, and to identify and stop potentially harmful incidents.” IDPSs are primarily used for identifying possible security incidents, recording all relevant information about them, attempting to respond to them, and reporting them to the proper cyber security administrators.

However, IDPSs often require significant manpower, and determining the best response is often very difficult. Successful monitoring requires on-going human effort and expertise, and sometimes the use of a collection of “home-brewed” tools. The results are that intrusion detection and response frequently do not operate in real time, meaning that significant damage may be done before detection and response occur.

Many high-quality tools, both open source and proprietary, exist for performing intrusion detection at a variety of levels. The most effective coverage combines detection based on malware signatures and anomalous patterns. These tools produce “alerts,” or indications that suspicious or prohibited activities have occurred, or at least occurred more frequently than chance would indicate. This information is fairly low level and high volume, detailing the specifics of each attack but not giving any immediately actionable information.

Unfortunately, these data are rarely combined with data that would allow security managers to understand the targets of attacks, attackers’ identities, attack strategies, and the amount of information compromised at a certain point in time. This desired output is high level and low volume; that is, the goal is the production of smart metrics that can be used to infer the nature or patterns of attacks and thereby trigger appropriate responses. The processing of low-level alerts into high-level intelligence, however, is quite challenging.[69] Additionally, smaller organizations lacking the manpower and expertise to do this for themselves may have to settle for a lower level of defensive capability or contract for expensive services from a service provider. Such a provider has to be trusted and will almost certainly lack an intimate understanding of the unique aspects of the customer’s organization and business model.

Several groups have worked on developing a standard for intrusion detection software. In 2007, the IETF developed a protocol called the Intrusion Detection Exchange Protocol, outlining the format of IDS output so that vendors can create IDS software compatible with other vendors’ software (Feinstein and Matthews, 2007). NIST has also previously contributed to IDPS technology in several ways, including the development of several recommendations

[69] According to security experts, tool support for this task is fair at best. An IDPS typically generates a high level of alerts—most systems are under constant attack from a variety of sources.

publications[70], the operation of the National Vulnerability Database, and the development of the Security Content Automation Protocol (SCAP).[71] Unfortunately, these standards and protocols do not specifically address the issue of information correlation and distillation.

6.6.1 Support from Interviews with Industry and Security Experts

Case study interviews and interviews with experts suggest that without automation, only a very small number of organizations, with large security departments and a high level of expertise, will be able to adequately detect and prevent threats. Several security experts noted that intrusion detection has most commonly been implemented in the form of basic antivirus and malware scanners, with limited adoption of more advanced tools. They also noted that standards could help to increase adoption. Further, most companies interviewed during case studies noted a gap in the availability of automatic defenses to combat a growing malware problem.

6.6.2 Market Failures Preventing Improved Automated Threat Detection and Prevention

There is lack of sufficient standardization among intrusion detection vendors because of a standard public-goods market failure and a coordination market failure. According to an article written for Symantec, intrusion detection software from different vendors will not work together, and “you cannot use one IDS interface to poll another vendor’s real-time data, easily correlate results, or seamlessly integrate alert management out of the box” (MacBride, 2010). This suggests cost inefficiency for companies that use several proprietary intrusion detection tools. Further, without widespread standardization, automation is largely impossible.

Given the significant increase in the level of malware, companies are struggling to keep current with new malware scanners and other software available to address the evolving threats. Reviewing and testing the multitude of new products is a very time-consuming process that requires a high degree of expertise, which is generally unavailable. This suggests an imperfect information market failure—there is an insufficient level and quality of data available with which to make investment decisions regarding threat detection technologies. Currently, the cost and time needed before a decision can be made is high, resulting in excessive transactions costs.

6.6.3 Recommended Improvements in the CSTI

One specific recommendation offered by a security expert would be for NIST to convene a meeting of practitioners to discuss what works and what is needed in this area. A major goal should be to encourage industry to meet this need and provide much greater automation of the

[70] NIST Special Publication 800-94 (NIST, 2007a) and Internal Report IR-7007 (NIST, 2003b) both offer valuable advice on selecting and configuring intrusion detection and prevention systems.

[71] SCAP consists of a variety of elements including Open Vulnerability Assessment Language, Open Checklist Interactive Language, Common Configuration Enumeration, Common Platform Enumeration, Common Vulnerabilities and Exposures, Asset Identification, Common Vulnerability Scoring System. For more information, see http://scap.nist.gov/index.html.

task of configuring, monitoring, and analyzing the results of intrusion detection, based on standardized methods. It would also be useful to identify the skills needed for operating such systems and perhaps to partner with industry and academia to broaden that skill base, perhaps by developing training materials or accreditation standards.

An initial step in this area of the CSTI should be a coordinated effort to evaluate the strengths and shortcomings of existing solutions. Publicly provided research could help identify optimal tools and approaches for intrusion detection/prevention, increasing private organizations' utilization of existing solutions, and could eventually increase the choices available in the future. As a result, the cost of effective defenses, for both small and large organizations, would be reduced. Moreover, the time required for recognizing and effectively responding to attacks would be reduced, the difficulty of processing intrusion detection outputs would be lessened, and the pool of persons qualified to operate IDPS systems would be increased.

6.7 Inadequate Protection and Mitigation from Loss of Equipment and Media

Although mobile security was discussed in Section 6.4, this section focuses on the physical security of mobile devices and media, whereas Section 6.4 focused primarily on securing mobile data through software-based methods. Often, companies lose data because actions by employees or contractors accidentally compromise the devices containing company data. Employees often misplace physical records, laptops, USB devices, and mobile devices, which can result in data loss.[72]

As the use of mobile devices becomes more prevalent, employees often use mobile phone, laptops, and tablet computers to store, access, and transmit company data. Although policy solutions can be used to help motivate employees to reduce the risks that they may lose a device, thus far, such solutions have not been sufficient. Technology solutions could be used to help organizations manage the use and location of their mobile devices, but currently the necessary infrastructure to support such technologies does not exist.

6.7.1 Support from Interviews with Industry and Security Experts

Several security managers interviewed during case studies specifically mentioned that lost and stolen laptops and mobile devices was their biggest security concern. One interviewee stated that most known data breaches were typically caused by lost devices. The overall consensus was that the biggest risk factor for negligent losses of data comes from mobile devices, the use of which exposes the company to a variety of potential losses. The CSTI gaps lie in a company's ability to protect, track, and control mobile devices remotely. Companies today

[72] Of note, the loss of a device is only considered a data breach if the device is unsecured. For instance, if an employee loses a laptop that is shut down and that laptop requires a login/ password, the loss may not be considered a breach because there is a reasonable guarantee that the data cannot be accessed by anyone who happens to find the laptop.

cannot track devices or physically limit where they may be taken. Moreover, if a device is lost, companies need to be able to remotely wipe the data. The companies we spoke with were generally not able to track or wipe devices[73]; however, they espoused the use of encryption to proactively protect devices from loss or theft. Unfortunately, simply protecting the devices and their wireless traffic seems to be insufficient.

Based on security experts' assessment of the current state of this gap, generic technology is needed to support the ability of technology providers to develop products and services that adequately monitor and secure mobile devices. The required investments are likely beyond an individual company's technical expertise and/or may require too large an investment.

6.7.2 Market Failures Preventing Improved Protection and Mitigation from Loss of Equipment and Media

The lack of sufficient tools to monitor and secure mobile devices is primarily the result of a public-goods market failure and a coordination market failure. Companies are not willing to invest the significant resources needed to improve their ability secure mobile devices through technology solutions because they may not retain all of the benefits of such. Further, the development of such solutions may require the coordination of expertise across organizations, for which a single company is not likely to have the skills or dollars to support.

6.7.3 Recommended Improvements in the CSTI

Because this data loss deals with mobile devices, many of the solutions involve mobile security, and there is significant overlap between this section and Section 5.2. To specifically counter the loss of company resources and data because of negligence, security experts interviewed noted that companies need solutions that offer specific controls for their resources. Broadly, areas of needed investment by organizations such as NIST include improving mobile device location and tracking capabilities and centralized remote administration and classification of data that are distributed across mobile devices.

The ability to track mobile devices and their data could help reduce the security risk of lost or stolen devices. This tracking ability would help prevent a lost device from turning into a data breach by enabling a company to recover or potentially destroy data on a device believed to be compromised. Although this type of service is offered by many mobile applications, interviews showed that a lack of trust prevents these solutions from being implemented. A significant concern, as mentioned before, is that the companies that track location data may use collected data for other purposes. This problem may be solved by a set of rules that must be followed by an organization that collects and uses mobile data. Organizations that provide

[73] Note that technology does exist that enables remote device wipe, but often the wipe is not permanent (Porter, 2012).

tracking services may be certified with a trusted label. A role for NIST would be the development of rules and certification procedures.

Another area for improvement is the remote administration and segregation of data that are remotely stored or accessed.[74] Data that are allowed to be remotely accessed or stored could be separately classified, and such data may be subject to limitations such as encryption requirements, sensitive information exclusion, and context-specific access. Moreover, data may be categorized into levels of risk, similar to the way in which transactions in federal agencies are mapped to a particular risk level and an appropriate NIST level of assurance. Each higher level of risk/assurance would have a stronger set of requirements. The highest level, for instance, may require that data be encrypted, transferred over a safe network, and accessed from an approved device using company-issued software. This infratechnology can promote the productive use of mobile devices by removing the uncertainty of the risks present in opening data for remote use.

6.8 Inadequate Education About IT Security Best Practices and Threat Awareness

Companies increasingly invest in employee education to promote security awareness; however, a significant gap in security awareness still remains. Companies are concerned about employees' risky behavior leading to data and privacy losses, but many are not taking substantive action to increase compliance with security best practices. In a PricewaterhouseCoopers survey (2011), just under half of respondents across North America required employees to complete privacy policy training and to certify compliance in writing, an increase from the prior year's survey.

Although many organizations have established procedures for protecting privacy, data, and assets, lack of employee compliance results in a concerning number of breaches. Informal and cultural awareness of security, implementation of frictionless or mandatory security controls, and enforcement of security accountability can all help improve security by discouraging activities that may result in losses to companies. Unfortunately, such information is often viewed as overly complicated or not sufficiently tailored to a company or industry, particularly by small businesses.

NIST has developed several publications in this area and recently is working in collaboration with the Department of Homeland Security on this topic. Special Publication 800-50, entitled *Building an Information Technology Security Awareness and Training Program*, explains how to design and implement a training program and develop training materials (NIST,

[74] Traditional security involves the building of basic defenses for data that have a securable physical perimeter, such as data stored centrally within a company or data center. However, in the case of distributed data, there is no perimeter, and data do not stay in one place. This necessitates a separate treatment of data that are stored or accessed remotely.

2003a). The recently initiated National Initiative for Cyber security Education, or NICE, being managed by NIST, in collaboration with DHS, aims to provide more help in this area.[75] Despite these efforts, the majority of organizations we interviewed expressed concern that developing best practice documents, particularly to help educate employees, is an area of significant need.

6.8.1 Support from Interviews with Industry and Security Experts

A study by the Ponemon Institute (2012) found that 87% of employees within U.S. companies are negligent in at least one area of cyber security. These areas of negligence are generally activities that circumvent established security tools, policies, or procedures. A number of factors influence employees' decision to circumvent established security controls. Our case study interviewees offered some ideas for reducing employee negligence.

Case study interviewees' biggest concern was the lack of a security-oriented culture, one in which cyber security would be an ethical, and not just a contractual, obligation. Another concern was security usability; one interviewee mentioned that employees typically disable security features that are important but optional during software installation. Another interviewee was concerned about a lack of incentives for or disincentives from protecting data. For example, employees who lose data through negligence need to be held accountable in some way.

6.8.2 Market Failures Preventing Improved Education About IT Security Best Practices and Threat Awareness

The lack of sufficient best practice documents is largely based on the public-goods nature of cyber security. Small organizations, in particular, lack the resources and incentives to invest sufficiently in developing or identifying best practices. As such, they often have inferior security. Further, excessive transactions costs can prevent them from being able to adequately screen a potential security consultant to fill this role.

More broadly, improving employee compliance also has a public-goods component. It could be very expensive to adequately research the best means by which to incentivize compliance and disincentivize noncompliance. In addition, an individual company is not likely to accrue the full benefits associated with such an investment.

6.8.3 Recommended Improvements in the CSTI

Solving the gap in education about IT security best practices and threat awareness is an issue of incentives, disincentives, and enforcement. To change employee culture to one of stronger security, companies must be able to track activities regarding compliance with security policies more easily. One potential solution suggested by several security experts is the

[75] More information on NICE can be found at http://csrc.nist.gov/nice/. Additionally, the National Cyber Security Alliance (NCSA), a non-profit organization funded primarily by DHS, is working to increase the cyber security awareness of individuals and organizations. See more information on NCSA at http://www.staysafeonline.org/.

implementation of disciplinary action for breaches of cyber security policies. The key would be to aid in the development of standard company security policies that better outline both specific expectations for employees (what exact behaviors are “unsafe”) and the repercussions of such unsafe behavior.

NIST could also work to develop of a set of guidelines to address current security risks such as those posed by the use of mobile devices and social networks, specifying how to influence employees’ threat awareness. Training materials on how employees can help to address current risks can improve organizations’ ability to maintain a higher level of security using existing technical controls. Broadly, NIST could develop and regularly maintain and update a variety of training materials that could be used by companies as well as cyber security service providers who offer training to companies. This would reduce the costs to these service providers and provide potential customers (companies) a way to trust the quality of their training materials.

6.9 Inadequate Standards for Meeting Auditing and Compliance Requirements

Throughout our case study interviews, the most commonly mentioned factor yielding inefficient cyber security spending was compliance with regulations and auditing. A variety of regulations are in place to enforce the confidentiality of customer data and mandate the notification of any compromise in customer privacy, including:

- The **Gramm-Leach-Bliley Act** mandates that financial institutions protect their customers’ data and inform their customers of the institutions’ data privacy policies.
- The **Health Insurance Portability and Accountability Act (HIPAA)** protects patients’ personal information and information on patient health status and history, health care provisioned, and payments made for health care.
- The **Sarbanes-Oxley Act (SOX)** mandates that all companies that report to the Securities and Exchange Commission (SEC) assess and report on their internal controls, including information security controls.

Compliance steps can be very involved, and regulations often mandate new procedures, resulting in new costs for companies. The CSTI to support efficient and effective compliance is currently inadequate, especially for companies who are required to comply with multiple regulatory requirements. Although regulations set privacy goals, they offer no guidance as to what a compliant privacy policy should look like, what measures would speak to that policy being in place, or anything akin to a reference architecture. In other words these regulations express a required state, but offer no concrete guidance as to what characterizes that state and how that state could be measured and monitored.

In analyzing the costs of compliance with SOX, a study conducted by the Office of Economic Analysis of the SEC found that labor costs are the biggest cost component of auditing and regulation compliance and that the overall costs of compliance are largest in the first year of compliance (SEC, 2009). The data suggest that the most critical area for a company is the initial adoption of information security compliance capabilities, especially with respect to optimizing processes to reduce labor expenditures.

6.9.1 Support from Interviews with Industry and Security Experts

A primary need is the streamlining of processes involved with complying with the specifications of multiple audits. Several interviewees noted that paying for multiple audits is inefficient and costly. One company mentioned having to fulfill five audits, many of which have overlapping requirements. Separate audits with overlapping requirements typically lead to redundancies in verifying each audit. By making labor-saving improvements in meeting multiple auditing requirements, companies can reduce the gap.

Additionally, according to our case study interviews, many companies believe that regulations require fixed and ongoing costs that do not always translate into a reasonable increase in security. Some organizations have gone as far as saying that certain processes mandated by regulations do not increase security at all.[76]

6.9.2 Market Failures Preventing Improved Standards for Meeting Auditing and Compliance Requirements

The primary barrier to an effective market for compliance is a lack of coordinated standards, or a coordination failure. A multitude of regulations affect many companies, and although the requirements are often overlapping, they are not standardized across the regulations. As such, companies spend significant resources interpreting and complying with the regulations.

6.9.3 Recommended Improvements in the CSTI

Solutions for reducing the cost of regulation and audits aim to bring down two types of costs. One type of cost is associated with the processes mandated by regulations, such as steps toward breach notification and remediation. Another type is the cost of complying with auditing requirements, such as verifying a checklist of processes and components that need to be in place. A potential solution offered by several security experts to reduce both of these costs would be the establishment of a common framework for fulfilling regulatory requirements. Some companies use a simple spreadsheet representing a checklist "matrix," in which each required process or task is mapped to one or more audits. This centralized mapping decreases redundancies, ensuring that tasks are not repeated. Developing a common framework for efficiently meeting multiple auditing requirements has potential to significantly increase organizational efficiency.

[76] Many companies interviewed noted that regulations require fixed and ongoing costs that do not always translate into a reasonable increase in security. Some organizations went so far as to say that certain processes mandated by regulations do not increase security at all.

6.10 Summary

The nine CSTI gaps identified by industry and discussed in this section provide a new frame to identify evaluate areas of investments. These gaps represent the primary areas of technical infrastructure need as communicated by industry cyber security managers, based on their opinions of current technical inadequacies. Table 6-2 provides a summary for each CSTI gap of whether the need is primarily for new infratechnology, generic technology, or both. Overall, organizations and security experts generally agreed on the nature and scope of the gaps, but not surprisingly, security experts were more willing (and likely more able) to provide specific recommendations for filling these gaps.

Several gap areas have significant overlap. The need for improved security metrics could help improve all of the other identified gaps. Mobile device security (focusing on software security) and protection from negligent loss of data and devices (focusing on physical security) overlap, and solutions in one could be used to improve the other. Education on best practices could benefit several other gaps, in particular protection from negligent loss of data and devices.

Recommendations for improvement broadly included the development of new standards, models, methodologies, policies, procedures and information sharing frameworks. Given the nature of these recommendations, NIST is uniquely suited to respond to or coordinate any action to be taken in response to these recommendations based on its mission, technical expertise, and ability to develop public-private partnerships. Other public and private organizations, including many discussed in Section 5, should support NIST in this role to ensure that new CSTI developed will be widely adopted.

Table 6-2. Primary Types of Technical Infrastructure Needed, by CSTI Gap Area

	Technical Infrastructure	
CSTI Gap Area	Generic Technologies	Infratechnologies
Authentication of all system users		●
Sharing of or access to threat data	●	●
Specification and collection of security metrics	●	●
Mobile device security		●
Cloud security	●	●
Automated threat detection and prevention	●	●
Protection and mitigation from loss of equipment and media		●
Education about IT security best practices and threat awareness		●
Standards for meeting auditing and compliance requirements		●

7. ECONOMIC BENEFITS OF IMPROVING THE CYBER SECURITY TECHNICAL INFRASTRUCTURE

This study quantified the economic benefits of narrowing nine CSTI gaps identified by private-sector cyber security directors as being the most important for near-term, targeted public or public-private investment. Analysis of a national survey of U.S. organizations revealed that the potential economic benefit to firms' cyber security operations would be $6.0 billion.

Following the methodology outlined in detail in Section 4, this prospective estimate of $6 billion in economic benefits was developed by pairing estimates of industry's willingness-to-pay for a 10% improvement in cyber security effectiveness with a set of specific improvements in the CSTI that, according to experts, would deliver those improvements. This section describes the survey sample, reviews survey respondents' willingness-to-pay estimates, and presents the extrapolated national impact estimates.

7.1 Survey Sample Characteristics

Although the survey (see Appendix A) was open to all respondents regardless of location, the sample used for economic impact estimation and summary statistics excluded non-U.S. organizations.[77] A total of 162 valid survey responses were received from U.S. respondents, 72% of which indicated that they were responsible for cyber security for their entire organization.

7.1.1 Industry, Revenue, and Employment Characteristics

Table 7-1 shows the distribution of responses by industry. 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.

To support comparison with the 2010/2011 Computer Security Institute (CSI) Computer Crime and Security Survey sample (Richardson, 2011), Text Box 7-1 compares our sample to the CSI sample and provides discussion of the representativeness of the data collected in this study.

[77] Appendix B provides data for domestic and international survey respondents, in the same format as tables in this section for U.S. respondents only.

Table 7-1. Industries Represented by RTI Survey Respondents

Industry	Number of Respondents	Percentage of Respondents	Percentage of Respondents from CSI Survey[a]
Finance and insurance	34	20.99	10.60
Information	24	14.81	10.90
Manufacturing	17	10.49	6.00
Professional, scientific, and technical services	19	11.73	21.50
Health care and social assistance	13	8.02	6.60
Educational services	8	4.94	8.90
Public administration	7	4.32	3.20
Retail trade	6	3.70	3.20
Utilities	11	6.79	
Other	23	14.20	
Total	**162**		

[a] Source: Richardson (2011).

Figures 7-1 and 7-2 present the distribution of survey respondents' organizations by size ranges for revenue and employment. Approximately 50% of responding organizations reported annual revenues of $250 million or greater in 2010, with nearly 35% reporting revenue of $1 billion or more (Figure 7-1). Twenty-nine percent employed fewer than 500 employees, 35% employed between 500 and 4,999 employees, and 36% employed more than 5,000 employees.

Table 7-2 presents the sample's mean, median, and total values for revenue and employment. Employment and revenue values were estimated by taking the midpoint estimation of closed ranges,[78] except for respondents that reported revenue equal to or greater than $1 billion and employment equal to or greater than 100,000. For these responding organizations, secondary industry data was used (Hoovers, 2012).[79] The median revenue was $297 million and median employment was 3,000. Collectively, the entire sample accounted for $641 billion in annual revenues and more than 3 million employees.

[78] See survey instrument in Appendix A, which includes several questions in which respondents were asked to choose between ranges of numbers (e.g., annual revenue).

[79] Hoovers data on U.S. company revenues and employment was used to estimate average revenue and employment for companies with greater than $1 billion in revenue and greater than 100,000 employees, in the industry in which the survey respondent self-identified.

Text Box 7-1.

Representativeness of the Survey Population

Absent robust data on the specific characteristics of all organizations in the survey population,[a] we could not accurately determine the statistical representativeness of the U.S. sampling population of 162 organizations to the survey population. However, the representativeness of the sampling population can be described by comparing characteristics of the respondent population with corresponding information derived from national statistics, other data sources, or other studies.[b]

To test representativeness of our data set, we compared the sample data from our survey with comparable data from the widely recognized Computer Security Institute (CSI) 15th Annual 2010/2011 Computer Crime and Security Survey (Richardson, 2011). CSI has conducted one of the longest-standing and most widely used surveys of organizational cyber security investments and perceptions of and behaviors surrounding cyber security threats. To illuminate cyber security investment trends, Gallaher, Link, and Rowe (2008) provided a summary of data from the CSI survey, which for the first 10 years was cosponsored by the Federal Bureau of Investigation (FBI).

To test for representativeness, we posited two hypotheses. The first hypothesis was that the distribution across industries in our survey sample and the distribution across industries in the CSI sample came from the same underlying distribution. See Table 7-1 for the underlying data. To test the first hypothesis, we calculated the Kolmogorov-Smirnov statistic. It equaled 0.22, and as such, the hypothesis of similar underlying distributions could not be rejected.[c]

The second hypothesis is that the distribution of cyber security spending as a percentage of total IT spending in our sample and the distribution of cyber security spending as a percentage of total IT spending in the CSI sample came from the same underlying distribution. Our data show that 41% of respondents spent 1–2% of their IT budgets on IT security, 24% spent 3–5% on IT security, 12% spent 8–10% on IT security, and 23% spent more than 10% on IT security. As above, comparing this distribution with that in the CSI sample, the Kolmogorov-Smirnov statistic is 0.50, and as such, the hypothesis of similar underlying distributions could not be rejected.

These analyses support the assertion that the data collected in this study are statistically similar to the data collected by the CSI survey, which provided the most widely used data on companies’ cyber security spending.

[a] The survey population for this study is all U.S. companies.

[b] As described in Section 4, our response rate was approximately 1.2% of companies directly contacted by RTI or organizations promoting the survey for RTI.

[c] This is not surprising. The Pearson correlation coefficient between the two distributions is 0.712, and it is significant at the 0.05-level.

Figure 7-1. Distribution of US Respondents by Revenues (2010)

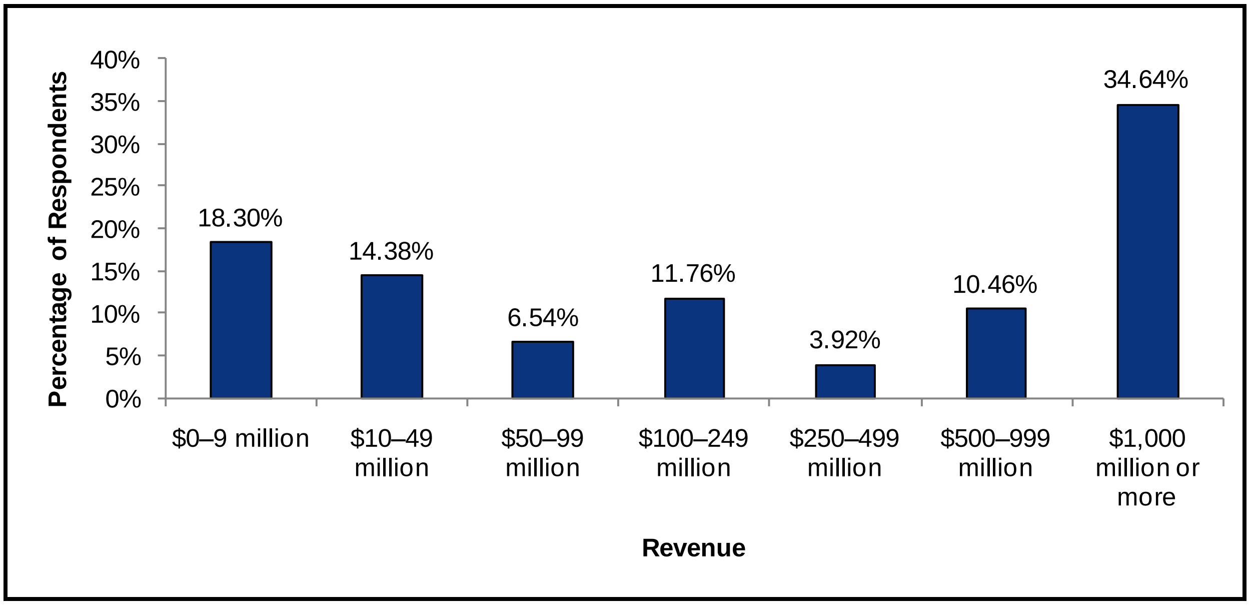


Figure 7-2. Distribution of U.S. Respondents by Number of Employees (2010)

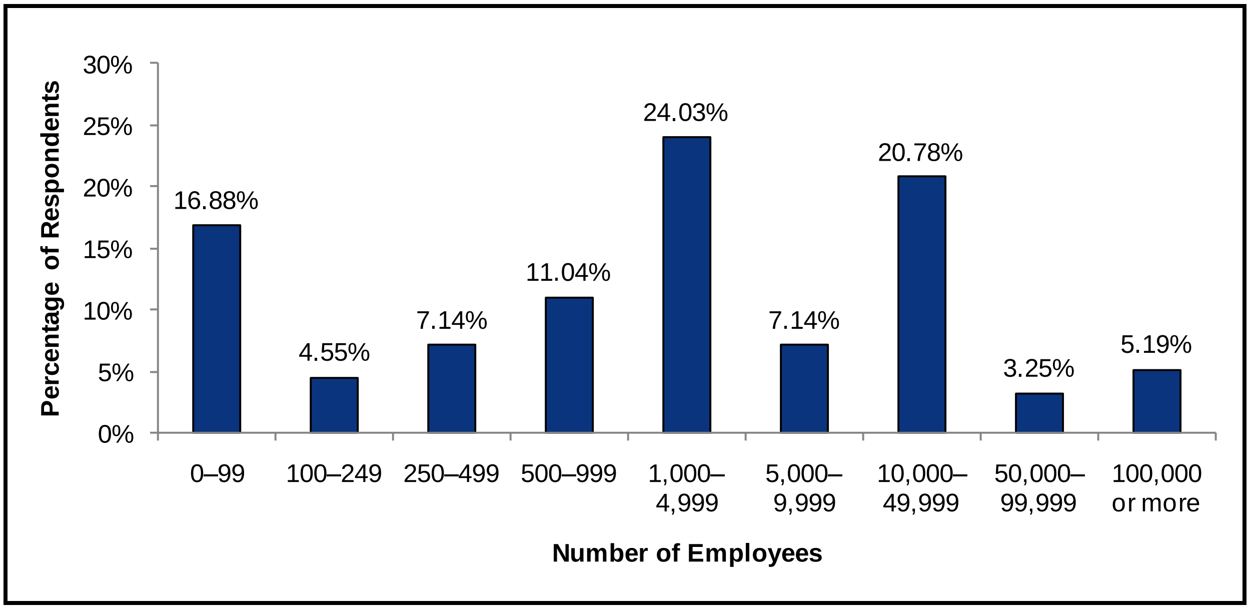


Table 7-2. Employment and Revenue of U.S. Respondents' Organizations (2010)

	n	Mean	Median	Total
Revenue	153	$4,189,171	$297,000	$640,943,113
Employment	154	21,279	3,000	3,064,738

7.1.2 Cyber Security Expenditures

Most organizations who responded to the survey (65%) spend less than 5% of their IT budgets on IT security, on an annual basis. Only 23% of organizations spend more than 10% on IT security, and 41% spend 1-2% on IT security. Figure 7-3 provides these data graphically.

Although the valuation method did not require it, to provide insight into the survey sample's characteristics, respondents were asked to distribute their annual cyber security budgets across the factors of production. On the average, as shown in Figure 7-4, they reported that 47% of their spending was for labor resources; 30% was for software, hardware, and other forms of capital; and 21% was for consulting and vendor services. Only 2% was characterized as some other form of expenditure. Respondents' breakout of their cyber security budgets is within 5% points of Gartner survey estimates for 2012 (Guevara, Hall, & Stegman, 2012), with the exception that capital expenditures reported by Gartner's respondents are about 10% larger than those reported in our survey.

Figure 7-3. Distribution of U.S. Respondents by IT Security Spending as a Percent of Total IT Spending (2010)

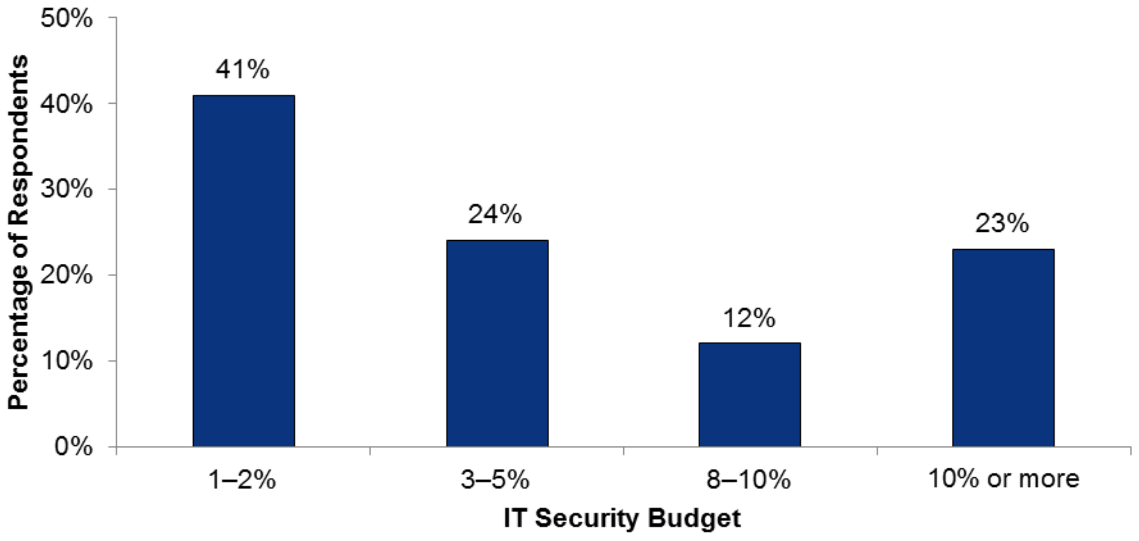
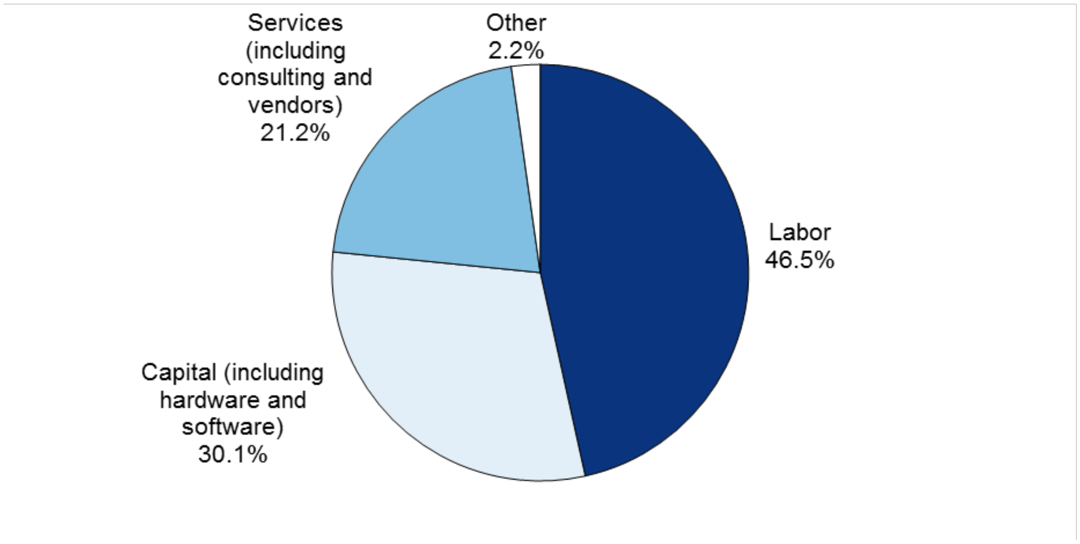
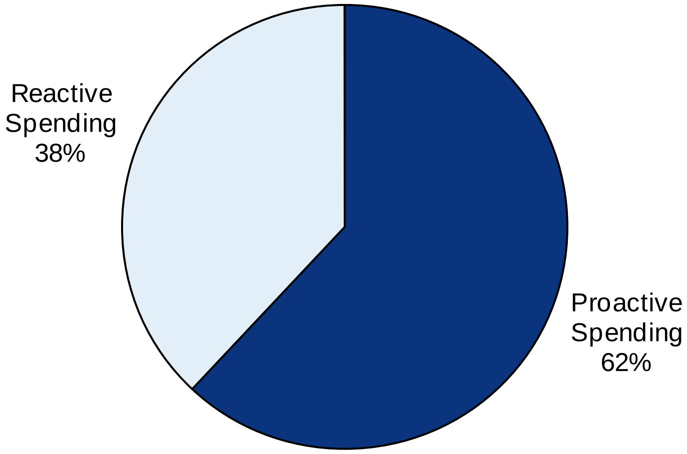


Figure 7-4. Distribution of Cyber Security Spending by Type (2010)



IT security directors often characterize their spending as “proactive” or “reactive,” and this survey indicated 62% of their security budget would be considered proactive and 38% reactive (Figure 7-5). *Proactive spending* covers expenditures on labor, capital, or services to help *avoid* incidents and breaches, while *reactive spending* covers expenditures made in *response to* incidents and breaches.

Figure 7-5. Cyber Security Spending: Proactive vs. Reactive (2010)



7.2 Economic Benefits of Narrowing CSTI Gaps: Survey Sample Analysis Results

Because CSTI is a nuanced topical area, respondents to the survey were asked a series of prospective questions about their willingness to pay for a 10% improvement in the effectiveness in nine key areas of their cyber security operations. (Willingness-to-pay is an approximation of benefits because, in theory, one's maximum willingness-to-pay should be equal to the expected benefits one would receive.) The key areas were the nine CSTI gaps private-sector cyber security directors identified in interviews as the most important to address, and they were also the gaps for which cyber security experts offered recommendations for how targeted CSTI investments could enhance the effectiveness of cyber security operations. Thus, as described in Section 4, the questions allowed us to determine the economic benefits organizations would accrue if gaps in the CSTI were narrowed.

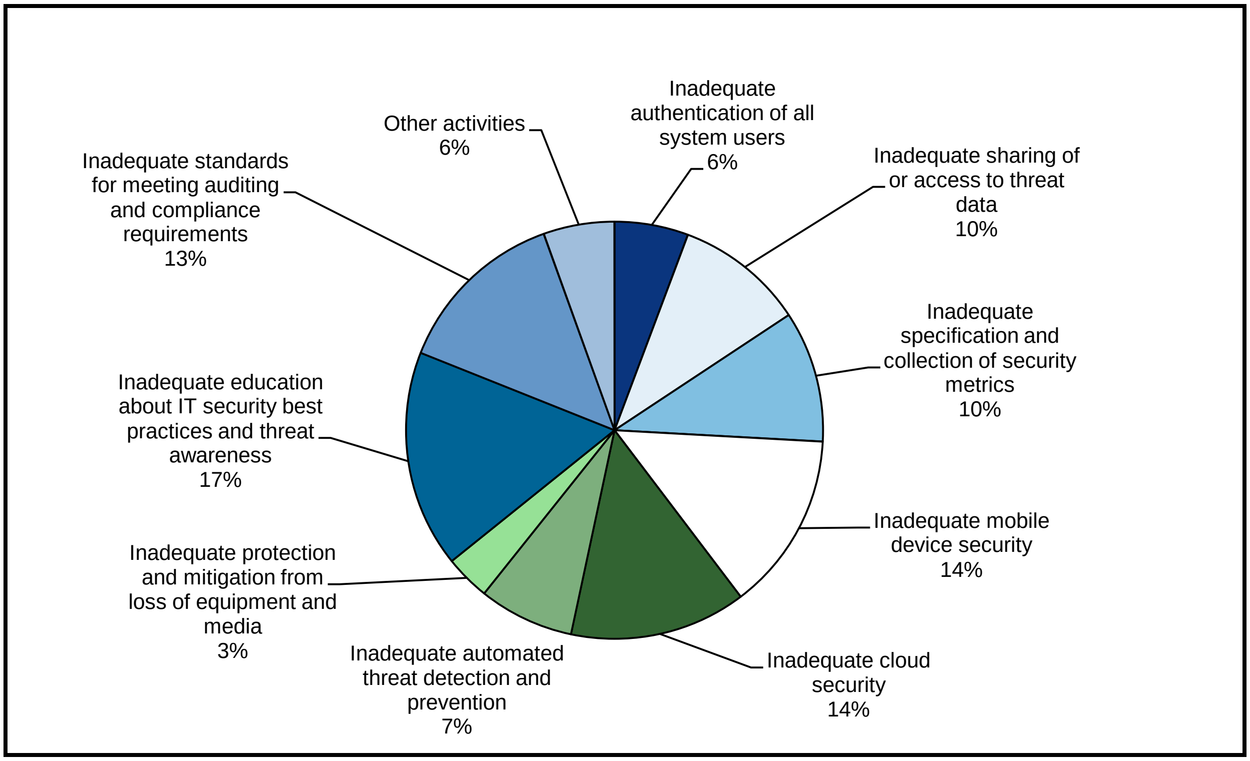
Respondents were asked to estimate the total amount they would be *willing to pay*, in terms of a percentage increase in their cyber security budgets, for a 10% increase in cyber security effectiveness, as measured in the percentage decrease in the number of security incidents or breaches. Table 7-3 summarizes the 108 responses received for this question. On average, companies indicated a willingness to spend approximately 14.7% of their cyber security budgets to increase their cyber security effectiveness by 10%. On average, the companies sampled were willing to spend approximately about $1 million.

To gauge how these benefits could be distributed among the nine CSTI gaps, respondents were asked to allocate a hypothetical 10% increase in their IT security budgets among the CSTI gaps plus an "other" category (if they would spend the money on areas other than the nine listed). Their responses, summarized in Figure 7-6, demonstrate a prioritization of CSTI-related activities. The *other* category turned out to be an insignificant priority, providing further justification that the key gap areas reflected critical priorities. The most important priorities, based on our survey response, were narrowing the gaps associated with education about IT security best practices and threat awareness, mobile device security, cloud security, and meeting auditing and compliance requirements.

Table 7-3. Willingness to Pay for a 10% Increase in IT Security Effectiveness per Respondent

Question	n	Mean Percentage of Cyber Security Budget	Mean Amount ($thousand)	Total Amount ($thousand)
As a percent of your IT Security spending, how much would you be willing to pay for a 10% improvement in your IT security effectiveness?	108	14.76%	$953	$98,202

Figure 7-6. Average Allocation of 10% Increase in Cyber Security Budget Among CSTI Gap Areas



Estimates of respondents’ spending priorities were used to deduce their willingness to invest in each of the nine areas to achieve a 10% increase in cyber security effectiveness. That is, for each respondent that contributed to the willingness to spend average in Table 7-3, their willingness to spend on each of the nine areas was found by multiplying the high-level willingness to spend and the percentage priority in each area in Figure 7-7. For instance, if a respondent is willing to pay 20% of her IT security budget for a 10% increase in IT security and would allocate 10% of this budget increase to authenticating all system users, her willingness to pay for a 10% increase in effectiveness of authenticating all system users would be 2% of her IT security budget (10% of 20% = 2%).

The resulting data on respondents’ willingness to spend in each area were multiplied by the provided cyber security budgets, and totals for all survey respondents and each of the six focus industries are shown in Table 7-4. These amounts represent only survey respondents’ valuation of cyber security improvements and are considered to be the monetary benefits of a 10% increase in CSTI-related cyber security effectiveness.

Figure 7-7. Overview of Extrapolation of Benefits to U.S. National Estimate

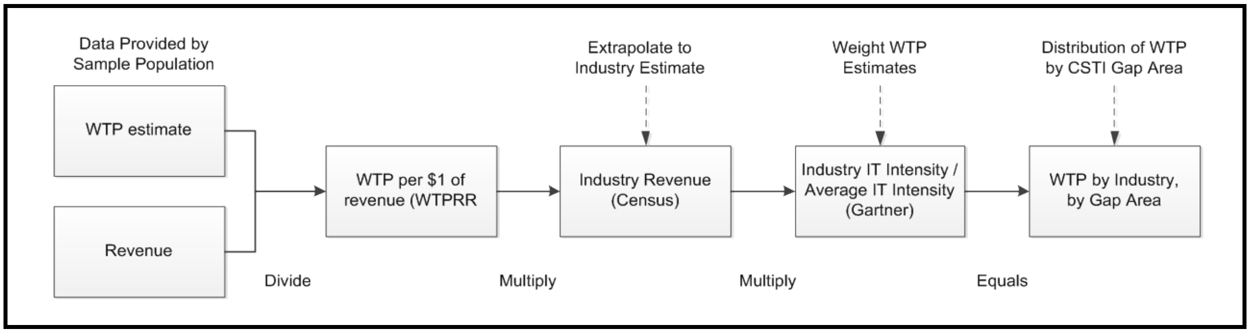

Data Provided by Sample Population
WTP estimate
Revenue
Divide
WTP per $1 of revenue (WTPRR
Multiply
Extrapolate to Industry Estimate
Industry Revenue (Census)
Multiply
Weight WTP Estimates
Industry IT Intensity / Average IT Intensity (Gartner)
Equals
Distribution of WTP by CSTI Gap Area
WTP by Industry, by Gap Area

Table 7-4. Estimated Benefits for a 10% Improvement in the CSTI by Gap Area, Surveyed Organizations Only ($thousand)

Gap Area	Information	Manufacturing	Finance and Insurance	Retail Trade	Health Care and Social Assistance	Utilities	Total (Key Industries)	Total (All Industries)
Cloud security	12,328	3,120	538	176	81	39	16,281	16,743
Mobile device security	9,578	912	688	119	81	37	11,413	13,567
Specification and collection of security metrics	4,584	1,520	867	22	5	8	7,007	9,768
Standards for meeting auditing and compliance requirements	4,515	1,543	847	35	5	56	7,001	9,610
Automated threat detection and prevention	5,712	768	1,821	9	7	41	8,358	9,252
Sharing of or access to threat data	3,652	735	2,274	9	5	11	6,685	9,215
Education about IT security best practices and threat awareness	3,675	2,938	752	46	158	37	7,605	8,554
Authentication of all system users	5,075	2,237	572	18	7	12	7,920	8,214
Protection and mitigation from loss of equipment and media	479	1,456	314	9	5	2	2,264	2,755
Total	**49,597**	**15,227**	**8,672**	**443**	**354**	**242**	**74,534**	**87,679**

Note: Sums may not add to totals due to independent rounding. Further, note that the total benefit estimates in this table do not match the total estimated benefits of a 10% improvement in in cyber security ($98,202), as presented in Table 7-3. The estimate in Table 7-3 includes additional benefits beyond those estimated to result from the nine CSTI improvements of focus in this study.

7.3 Economic Benefits of Narrowing CSTI Gaps: National Impact Estimates

The combined revenue of the 162 survey respondents was equivalent to about 4.54% of gross domestic product (GDP) As described in Section 4, industry-specific revenue data from U.S. Economic Census and IT intensity data from Gartner were used to extrapolate the willingness-to-pay (benefit) estimates from the survey sample to national benefit estimates (see Figure 7-6). Table 7-5 presents revenue and IT intensity data for 2012 used in the extrapolation procedure.

Table 7-5. U.S. Industry Revenues and IT Intensity (2012)

Industry	2012 Revenue[a.b] ($ million)	2012 IT Intensity[c,d]
Mining, quarrying, and oil and gas extraction	456	1.00%
Utilities	644	2.40%
Construction	1,908	1.00%
Manufacturing	5,861	1.90%
Wholesale trade	7,179	1.30%
Retail trade	4,317	1.30%
Transportation and warehousing	705	2.70%
Information	1,182	5.55%
Finance and insurance	4,043	4.75%
Real estate and rental and leasing	534	4.30%
Professional, scientific, and technical services	1,378	4.30%
Management of companies and enterprises	115	4.30%
Administrative and support and waste management and remediation services	695	4.30%
Educational services	50	4.50%
Health care and social assistance	1,838	3.10%
Arts, entertainment, and recreation	209	4.10%
Accommodation and food services	676	1.20%
Other services (except public administration)	447	4.50%
Total	**32,236**	

[a] Economic Census (U.S. Census Bureau, 2007b).

[b] 2007 revenue converted to 2012 using the consumer price index (CPI) from BLS (2012a).

[c] Gartner (2012).

[d] IT intensity equals IT spending as a percent of revenue.

Note: Sums may not add to totals due to independent rounding.

Per the estimation procedure detailed in Section 4, we estimated the total wiliness to pay for each CSTI gap per dollar of revenue by summing each survey respondent's deduced willingness to pay per dollar of revenue for narrowing each CSTI gap. Next, weighted willingness-to-pay estimates per dollar of revenue (WTPR) for each CSTI gap were extrapolated to national estimates for each industry. WTPR multiplied by industry revenue and the industry's IT intensity factor yielded industry specific benefits estimates, the sum of which are the national benefit estimates.

Table 7-6 shows the resulting prospective economic impact of narrowing CSTI gaps by 10%. We estimated that the total benefits accruing to the cyber security operations of U.S firms to be approximately $6.0 billion. Based on follow-up interviews with U.S. organizations that provided survey data, the estimated benefits of new cyber security infrastructure are likely to accrue over approximately a 4-year period on average,[80] with more benefits received in the first year ($2.2 billion) than in later years. As shown, the largest 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).

Table 7-7 presents impact estimates for six industries—finance, health care, retail, utilities, information, and manufacturing—which as a group would accrue $3.7 billion of the expected benefits. The most benefit will accrue to the finance industry ($1.3 billion) followed by the manufacturing industry ($967 million), with the utilities industry receiving the least benefit ($117 million).

[80] Interview participants suggested that when they make investments in new security products, services, or internal labor or policy changes, they typically assume a 4-year benefit. When we asked about the likely spread of benefits from improved CSTI and mentioned RBAC as an example, on average firms estimated a 4-year spread of the benefits.

Table 7-6. Estimated Benefits for a 10% Improvement in the CSTI per Year, Extrapolated to Total U.S. ($ million)

Gap Area	2012	2013	2014	2015	Total
Cloud security	430	322	243	150	1,146
Mobile device security	349	261	197	122	928
Specification and collection of security metrics	251	188	142	88	668
Standards for meeting auditing and compliance requirements	247	185	140	86	658
Automated threat detection and prevention	238	178	134	83	633
Sharing of or access to threat data	237	177	134	83	631
Education about IT security best practices and threat awareness	220	164	124	77	585
Authentication of all system users	211	158	119	74	562
Protection and mitigation from loss of equipment and media	71	53	40	25	189
Total	**2,255**	**1,687**	**1,275**	**790**	**6,000**

Note: Sums may not add to totals due to independent rounding.

Table 7-7. Estimated Benefits 2012–2015 for a 10% Improvement in the CSTI, Extrapolated to Total U.S. ($ million)

Gap Area	Finance and Insurance	Manufacturing	Retail Trade	Health Care and Social Assistance	Information	Utilities	Total (Key Industries)	Total (All Industries)
Cloud security	256	185	84	82	80	22	709	1,146
Mobile device security	208	150	68	66	65	18	575	928
Specification and collection of security metrics	150	108	49	48	47	13	414	668
Standards for meeting auditing and compliance requirements	147	106	48	47	46	13	407	658
Automated threat detection and prevention	142	102	47	45	44	12	392	633
Sharing of or access to threat data	141	102	46	45	44	12	390	631
Education about IT security best practices and threat awareness	131	94	43	42	41	11	362	585
Authentication of all system users	126	91	41	40	39	11	348	562
Protection and mitigation from loss of equipment and media	42	30	14	13	13	4	117	189
Total	**1,342**	**967**	**441**	**429**	**418**	**117**	**3,715**	**6,000**

Note: Sums may not add to totals due to independent rounding.

8. CONCLUSION

The study projected economic benefits to U.S. industries of $6 billion if cyber security incidents and breaches were reduced by 10% following the introduction of new CSTI technologies. This finding is the culmination of an 18-month study that engaged cyber security directors at major corporations, security experts, and others about the role CSTI plays in promoting cyber security, what CSTI gaps are the most pressing from an economics perspective, and what would be the consequent economic impact of successful outcomes of targeted public or public-private R&D in CSTI gap areas.

The benefit estimates in Table 8-1 offer a guide to government agencies, policy makers, industry consortia, and the private sector for determining how to most efficiently allocate scarce CSTI investment resources. This study provides economic research that complements past and ongoing technical and policy reviews, adding a new perspective to support programmatic planning. As reported in Section 5, national CSTI investment amounted to approximately $716 million in 2012. The benefits estimated suggest that additional investments in the CSTI could have a significant positive economic impact on U.S. organizations, and although not quantified in the study, the amount of CSTI investment needed to achieve these benefits would likely be much less than the benefits that would result.

8.1 Prioritizing Future Investments in the CSTI

Table 8-2 summarizes a specific set of CSTI improvements that participating cyber security experts believe could improve cyber security effectiveness by at least 10% in the gap areas identified by industry. Both industry interviews and interviews with security experts suggested the need for new standards to describe critical cyber security metrics and developing new methodologies for using security metrics to identity levels of risk as critical. Proprietary metrics and methodologies and several open standards exist, but widespread adoption has been hampered by interoperability, ease of use, and lack of widespread agreement/acceptance.

Cloud security ($1.1 billion) and mobile security ($928 million) represent areas of significant need as represented by the magnitude of estimated economic benefits in these two CSTI gap areas. Although the benefits estimated are large, perhaps the potential economic impact of improving mobile and cloud security would actually be much greater. Survey data collected from industry suggests that improvements in cloud and mobile security would increase organizations’ use of cloud storage and applications by at least 30% and increase organizations’

Table 8-1. Total Estimated Benefits of a 10% Improvement in the CSTI, by Gap Area ($ million)

Gap Area	Total Benefits
Cloud security	1,146
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
Sharing of or access to threat data	631
Education about IT security best practices and threat awareness	585
Authentication of all system users	562
Protection and mitigation from loss of equipment and media	189
Total	**6,000**

Note: Sums may not add to totals due to independent rounding.

use of mobile technologies by 30% (Table 8-3).[81] Our interviews with industry and security experts, supplemented by numerous popular press articles, suggest that increased use of mobile technologies and cloud technologies are high priorities for many companies looking to reduce infrastructure costs (a feature offered by cloud technologies) and increase staff productivity (a feature offered by mobile technologies). Additional economic benefits will likely result if security improvements increase companies' adoption of cloud and mobile technologies.

Although this study focused on the benefits to IT departments,[82] future investments in the CSTI should aim to leverage information on the broader benefits to organizations. Qualitatively, the benefits of organizations having a higher level of cyber security and/or decreasing spending on cyber security as a result of an improved CSTI could result in both productivity and efficiency improvements across organizational departments. Further, the recommended CSTI investments could increase the level of cyber security of organizations by more than 10%, resulting in larger economic benefits. As such, benefits estimated in this study should be viewed as minimum estimate of the total benefits that would accrue as a result of a 10% increase in cyber security based on an improved CSTI.

[81] Note that these figures combine information on the number of companies who indicated that they would increase their use of mobile and cloud technologies and, of those, the number of companies who provided information on the level of increased use.

[82] During the case study interviews, it was determined that IT security managers generally neglect to consider the total impact of cyber security on their organizations. This finding is consistent with past research on the costs associated with cyber security, which are very difficult to quantify. No past studies have succeeded in applying a rigorous methodology to quantify the non-IT costs of cyber security threats, attacks, and solutions.

Table 8-2. Recommended CSTI Improvements by Gap Area

Gap Area	Cyber Security Technical Infrastructure Examples
Cloud security	• Standard for specifying and/or certifying a cloud provider’s security policy and security offerings • Risk-assessment framework for cloud providers • Model of liability agreed upon by the cloud provider
Mobile device security	• Standard specifications for antivirus protection for mobile devices • Controls on minimum security capabilities for mobile devices/portable media • Usable mobile authentication standards
Specification and collection of security metrics	• Standards to describe metrics in a vendor-independent format • Improved methodology for risk-management-based cyber security
Standards for meeting auditing and compliance requirements	• Standard to map multiple auditing or compliance checklists into one centralized “matrix”
Automated threat detection and prevention	• Recommendations for intrusion detection deployment and operation • Framework for a crowd-sourced or outsourced incident investigation • Tools for helping with the processing of alerts • Standard metrics for intrusion detection and benchmarking
Sharing of or access to threat data	• Standards and protocols for the format of data being shared • Establishment of a trusted broker that can handle collection and dissemination of data • Standard legal agreement for making data anonymous and sharing data
Education about IT security best practices and threat awareness	• Best practices recommendations tailored for companies • A high-quality security training standard for end users and management in order to reduce susceptibility to attacks like phishing and social engineering
Authentication of all system users	• Standards for single sign-on • Standards for multifactor authentication, including combinations of strong passwords, hardware tokens, biometrics • Policies to support better data sharing among companies and thus enable risk-based authentication through context awareness
Protection and mitigation from loss of equipment and media	• Standards for improved mobile device tracking/wiping capabilities • Standard procedures to support centralized and remote administration of data that are stored or accessed from distributed devices

Table 8-3. Increase in Mobile and Cloud Computing Use if Security Was Guaranteed

Metric	Value
Mobile Devices	
Would your company increase use of mobile devices with guaranteed security?	54.74% Yes
If *Yes*, by how much would you increase use of mobile devices?	46.94%
Cloud Computing—Storage and Applications	
Would your company increase use of cloud computing with guaranteed security?	59.57% Yes
If *Yes*, by how much would you increase use of cloud storage?	44.20%
If *Yes*, by how much would you increase use of cloud applications?	40.98%

8.2 The Need for Public and Public-Private Partnership Support for the CSTI

As the number, complexity, and potential impact of cyber threats continue to increase, increased public sector involvement and public-private partnerships is essential. Given the public-good nature of the CSTI, the private sector is likely to underinvest in the CSTI from a social perspective. Individual firms' production of security depends on the total amount of the CSTI in society, resulting in firms' free riding because investments in the CSTI benefit multiple firms. Further, private firms do not consider the impact of their provision of the CSTI on other firms' ability to produce security, and as such, they undervalue the external benefits, or externalities, of their investments. Additional market failures affect private sector firms' ability to invest efficiently in the CSTI. For example, a coordination market failure and interoperability concerns arise when coordination and widespread consensus is needed for specific CSTI to be successful. NIST and other government agencies are well suited to invest more efficiently.

The need for government to provide support to industry for the development of the CSTI is analogous to the need for public sector support for public health, and this comparison offers a useful strategy for future CSTI investments.[83] From a public health perspective, in communicable diseases, if one person becomes sick the entire population may ultimately be at risk. Similarly in cyber security, a single hijacked computer or network can put many others at risk. In the case of the public health technical infrastructure, the government makes investments aimed at improving the availability of information on public health threats and potential solutions through research on, for example, new epidemiological models and metrics for measuring health outcomes.[84] Such

[83] Mulligan and Schneider (2011) suggest that cyber security should be approached like public health.

[84] A Department of Homeland Security white paper entitled *Enabling Distributed Security in Cyberspace Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action* (2011c) describes specific areas in which a public health model for cyber security is useful. Further, Rowe et al. (2012) delineate how a public health framework could be used to develop new cyber security evaluation methodologies for cyber security threats, solutions, and implementation strategies.

technical infrastructure helps individuals and organizations be more productive and helps health care organizations be more efficient. Similarly, as identified in this study, the government should make targeted investments in the CSTI—such as developing standards, defining metrics, and creating models—that increase the efficiency of cyber security investments made by all organizations.

Past studies of the role of technical infrastructure suggest that the public sector has higher productivity in producing the CSTI than individual companies do. Public institutions such as NIST have core expertise in developing technical infrastructure components, such as components of the CSTI, as compared with private firms, whose expertise is focused on their business model. See, for example, Gallaher et al. (2007). Thus, the public provision of the quasi-public goods is the preferred policy option.

Public investment would likely "crowd in" private-sector investment by making the private sector's investment more efficient. Collectively, CSTI components raise the level of national cyber security. They support efficiency in cyber security operations and stimulate innovation and competitiveness in the industries that produce related security products and services. The CSTI increases firms' return on cyber security R&D and increases customers' willingness to pay for products and services. In other words, targeted CSTI investments stimulate the deployment and diffusion of new technologies.

REFERENCES

Adams, J.T. 2011. 2011 *Budget Allocation Requests. Kantara Initiative*. Retrieved from: http://kantarainitiative.org/confluence/display/LC/2011+Budget+Allocation+Requests.

Air Force. February 2011. *Department of Defense Fiscal Year 2012 Budget Estimates: Air Force Justification Book Volume 2: Research, Development, Test & Evaluation, Air Force.* Retrieved from: http://www.saffm.hq.af.mil/shared/media/document/AFD-110211-030.pdf.

Anderson, Gary. 2012. "A Simple Model of Technical Infrastructure: The Importance of Technical Infrastructure and the Role of Government." NIST mimeo.

Anderson, Ross, Chris Barton, Rainer Bohme, Richard Clayton, Michel J.G. van Eetan, Michael Levi, Tyler Moore, and Stefan Savage. 2012. "Measuring the Cost of Cybercrime." Presented at the Workshop on the Economics of Information Security, Berlin, Germany. Retrieved from http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

Army Justification. Department of Defense. February 2011. *Fiscal Year (FY) 2012 Budget Estimates: Book Volume 1: Research, Development, Test & Evaluation.* Retrieved from: http://asafm.army.mil/Documents/OfficeDocuments/Budget/BudgetMaterials/FY12/rforms/vol1.pdf.

Badger, L., T. Grance, R. Patt-Corner, and J. Voas. May 2011. *Draft Cloud Computing Synopsis and Recommendations*. Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf.

Booz Allen Hamilton. May 19, 2009. *Mobile Device Security: NIST HIPAA Conference.* Retrieved from: http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/7-051909-new-technologies-mobile-devices.pdf.

Braden, J.B., C.D. Kolstad, C.D., J.A. Machado, and R.A. Woock. 1997. *Demand for synthetic fuels: Contingent valuation of quality-differentiated factors of production*. University of California at Santa Barbara, Economics Working Paper Series. Retrieved from http://www.econ.ucsb.edu/papers/wp08-97.pdf.

Bureau of Consumer Protection. n.d. In Brief: *The Financial Privacy Requirements of the Gramm-Leach-Bliley Act.* Retrieved from: http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act.

Bureau of Labor Statistics. 2012b. *Occupational Employment Statistics*. Retrieved from: http://www.bls.gov/oes/.

Bureau of Labor Statistics. 2012c. *Current Employment Statistics*. Retrieved from: http://bls.gov/ces/.

Bureau of Labor Statistics. February 17, 2012a. *Consumer Price Index: All Urban Consumers.* Retrieved from: ftp://ftp.bls.gov/pub/special.requests/cpi/cpiai.txt.

Center for Internet Security. n.d. *Overview & mission.* Retrieved from: http://www.cisecurity.org/about/.

Center for Strategic and International Studies (CSIS). 2008. *Securing Cyberspace for the 44th Presidency*. Retrieved from: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Center for Strategic and International Studies (CSIS). 2010. *Cybersecurity Two Years Later.* Retrieved from: http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

Champ, P., K. Boyle, and T.C. Brown. 2003. *A Primer on Nonmarket Valuation.* Dordrecht: Kluwer Academic Publishers.

Cloud Security Alliance. n.d. "Research Overview." Retrieved from: https://cloudsecurityalliance.org/research/.

Comptroller/CFO, Office of the Under Secretary of Defense. February 2011. *United States Department of Defense Fiscal Year 2012 Budget Request: Overview*. Retrieved from: http://comptroller.defense.gov/defbudget/fy2012/FY2012_Budget_Request_Overview_Book.pdf.

Constantin, Lucian (IDG News Service). March 28, 2012. Security Firms Disable the Second Kelihos Botnet. *PCWorld*. Available at: http://www.pcworld.com/article/252763/security_firms_disable_the_second_kelihos_botnet.html

CSO Magazine. 2010. *2010 "C*yberSecurity Watch Survey—Survey Results." Retrieved from: http://www.csoonline.com/documents/pdfs/2010CyberSecurityResults.pdf.

Davis, L.M., D. Golinelli, R. Beckman, S.K. Cotton, R.H. Anderson, A. Bamezai, C.R. Corey, M. Zander-Cotugno, J.L. Adams, R. Euller, and P. Steinberg. 2008. *National Computer Security Survey: Final Methodology*. Prepared for the Bureau of Justice Statistics. Santa Monica, CA: RAND. Retrieved from: http://www.rand.org/pubs/technical_reports/2008/RAND_TR544.pdf.

Deering. S., and R. Hinden. 1995. *Internet Protocol, Version 6 (IPv6) Specification RFC 1883*. Submitted to the Internet Engineering Task Force.

Defense Advanced Research Projects Agency (DARPA). Department of Defense. February 2011. *Justification Book Volume 1: Research, Development, Test & Evaluation, Defense Wide. Fiscal Year (FY) 2012 Budget Estimates.* Retrieved from: http://comptroller.defense.gov/defbudget/fy2012/budget_justification/pdfs/03_RDT_and_E/DARPA.pdf.

Defense Advanced Research Projects Agency (DARPA). May 2012. *Information Innovation Office.* Retrieved from: http://www.darpa.mil/Our_Work/I2O/.

Domenic, Helen and Afzal Bari. *The Price of Cybersecurity: Big Investments, Small Improvements.* January 31, 2012, Bloomberg Government.

Electric Light and Power (ELP). May/June 2008. *Cyber Security: Are We Doing Enough*? Volume 86, 03. Retrieved from: http://www.elp.com/index/display/article-display/330162/articles/electric-light-power/volume-86/issue-3/features/cyber-security-are-we-doing-enough.html.

Electricity Consumers Resource Council (ELCON). 2004. *The Economic Impacts of the August 2003 Blackout*. Retrieved from: http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf.

Ernst & Young. 2010. *Borderless Security; Ernst & Young's 2010 Global Information Security Survey*.

Feinstein, B., and G. Matthews. March 2007. *The Intrusion Detection Exchange Protocol.* Retrieved from: http://www.rfc-archive.org/getrfc.php?rfc=4767.

Financial Services Information Sharing and Analysis Center (FS-ISAC). 2011. *About the FS-ISA.* Retrieved at http://www.fsisac.com/about/.

Florencio, Dinei and Cormac Herley. 2011. "Sex, Lies, and Cyber-crime Surveys." Presented at the Workshop on the Economics of Information Security, Fairfax, VA. Retrieved from http://weis2011.econinfosec.org/papers/Sex,%20Lies%20and%20Cyber-crime%20Surveys.pdf.

Forum of Incident Response and Security Teams. n.d. Retrieved from: http://www.first.org/.

Gallaher, Michael, Jeffrey Petrusa, Alan O'Connor, and Stephanie Houghton. *Economic Analysis of the Technology Infrastructure Needs of the U.S. Biopharmaceutical Industry*. Prepared for the National Institute of Standards and Technology. Retrieved from http://www.nist.gov/director/planning/upload/report07-1.pdf.

Gallaher, M.P., A.N. Link, and B. Rowe. 2008. *Cyber Security: Economic Strategies and Public Policy Alternatives*. Cheltenham, UK, Northampton, MA: Edward Elgar Publishing.

Gartner. 2012. IT Metrics: *IT Spending and Staffing Report, 2012.* Stamford, CT: Gartner Report.

Greenberg, Andy (Forbes Staff). August 2, 2012. "Cybersecurity Bill's Backers Cite Antivirus Firms' Bogus Cybercrime Stats." Available at: http://www.forbes.com/sites/andygreenberg/2012/08/02/cybersecurity-bills-backers-cite-antivirus-firms-bogus-cybercrime-stats/

Guevara, J. K., L. Hall, L., and E. Stegman. 2012. *IT Key Metrics Data 2012: Key Information Security Measures: Current Year.* Stamford, CT: Gartner Report.

Guidestar. n.d. Retrieved from: http://www2.guidestar.org/.

Hoovers. 2012. Data obtained directly from Hoovers database on all U.S. company revenue and employment.

Horowitz, B.T. April 13, 2012. "Utah Health Care Data Breach Exposed About 780,000 Patient Files." eWeek.com. Retrieved from: http://www.eweek.com/c/a/Health-Care-IT/Utah-Health-Care-Data-Breach-Exposed-About-780000-Patient-Files-189084/.

ICF Consulting. 2003. *The Economic Cost of the Blackout*. Fairfax, VA: ICF Consulting. Retrieved from: http://www.solarstorms.org/ICFBlackout2003.pdf.

Information Security Forum (ISF). 2007. *The Standard of Good Practice for Information Security*. Retrieved from: https://www.securityforum.org/userfiles/public/SOGP.pdf. As obtained on February 4, 2001.

Information Systems Security Association. n.d. "Developing and Connecting Cybersecurity Leaders Globally." Retrieved from: https://issa.org/page/?p=Profile_16.

Internal Revenue Service. (2012) *Filing Season Statistics for Week Ending June 8, 2012.* Retrieved from http://www.irs.gov/uac/Filing-Season-Statistics-for-Week-Ending-June-8,-2012.

Internet Engineering Task Force (IETF). 2000. *Internet Security Glossary*. Retrieved from: http://tools.ietf.org/html/rfc2828.

Internet Society. n.d. "Security." Retrieved from: http://www.internetsociety.org/what-we-do/issues/security.

ISACA. 2012. "2011 Annual Report." Retrieved from: http://www.isaca.org/about-isaca/Pages/default.aspx.

ISACA. n.d. "About ISACA." Retrieved from: http://www.isaca.org/about-isaca/Pages/default.aspx.

Jansen, W. April 2009. *Directions in Security Metrics Research*. Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf.

Loomis, John. 2011. "What to Know about Hypothetical Bias in Stated Preference Valuation Studies." *Journal of Economic Surveys*, Vol. 25 (2), 363-370.

Lovelock, J. D., K. F. Brant, S. Cournoyer, R. L. Goodwin, V. K. Liu, C. Moore, J. Rooster, Shiga, R. Sood, and D. N. Finkeldey. 2009. Dataquest Alert: *Utilities, Healthcare and Government Lead IT Spending Growth in Challenging 2009*. Stamford, CT: Gartner Report.

MacBride, R. November 3, 2010. "Intrusion Detection: Filling in the Gaps." Mountain View, CA: Symantec. Retrieved from: http://www.symantec.com/connect/articles/intrusion-detection-filling-gaps.

Messmer, Ellen. July 22, 2009. “America's 10 Most Wanted Botnets: Ranked by Size and Strength, These Are the 10 Most Damaging Botnets in the U.S.” *Network World*. Available at: http://www.networkworld.com/news/2009/072209-botnets.html.

Miller, J. May 14, 2010. “DHS Tries Sharing Cyber Threat Data Differently.” *Federal News Radio*. Retrieved from: http://www.federalnewsradio.com/?nid=697&sid=1957093.

Mulligan, D. K. and F.B Schneider. “Doctrine for Cybersecurity.” *Daedalus*. Fall 2011, Vol. 140, No. 4, pages 70-92.

Nakashima, E. May 25, 2009. “Defense Department Joins Forces with Industry Against Cybercrime.” *The Washington Post*. Retrieved from: http://www.washingtonpost.com/wp-dyn/content/article/2009/05/24/AR2009052402140_pf.html.

National Council of ISACs. n.d. Information Sharing and Analysis Centers (ISAC). Retrieved from: http://www.isaccouncil.org/index.php?option=com_content&view= article&id=87&Itemid=194.

National Cyber-Forensics & Training Alliance. n.d. *About the NCFTA.* Retrieved from: http://www.ncfta.net/about-ncfta.

National Institute of Standards and Technology (NIST). 2002. The Economic Impacts of Inadequate Infrastructure for Software Testing. Prepared by RTI. May 2002. Retrieved from Available at http://www.nist.gov/director/planning/upload/report02-3.pdf.

National Institute of Standards and Technology (NIST). 2003a, October. *Building an Information Technology Security Awareness and Training Program*. NIST Special Publication 800-50. (Authors: Mark Wilson and Joan Hash). Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

National Institute of Standards and Technology (NIST). 2003b, February. *An Overview of Issues in Testing Intrusion Detection Systems*. Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/publications/nistir/nistir-7007.pdf.

National Institute of Standards and Technology (NIST). 2007a, February. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

National Institute of Standards and Technology (NIST). 2007b. *Mobile Devices*. Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/groups/SNS/mobile_security/mobile_devices.html.

National Institute of Standards and Technology (NIST). 2008, October. *Guidelines on Cell Phone and PDA Security: Recommendations of the National Institute of Standards and Technology.* Special Publication 800-124. (Authors: Wayne Jansen and Karen Scarfone). Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf.

National Institute of Standards and Technology (NIST). 2009, August. *Recommended Security Controls for Federal Information Systems and Organizations*. Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

National Institute of Standards and Technology (NIST). 2011a, February. *Ensuring a Secure and Robust Cyber Infrastructure*. Gaithersburg, MD: NIST. Retrieved from: http://www.nist.gov/public_affairs/factsheet/cybersecurity2012.cfm.

National Institute of Standards and Technology (NIST). 2011b, September. *The NIST Definition of Cloud Computing*. Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

National Institute of Standards and Technology (NIST). 2011c. *Guidelines on Security and Privacy in Public Cloud Computing*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology (NIST). 2012a. *National Cybersecurity Center of Excellence: Advancing Cybersecurity, Enhancing Economic Growth*. Retrieved from: http://www.nist.gov/public_affairs/factsheet/upload/nccoe.pdf.

National Institute of Standards and Technology (NIST). 2012b. *Guidelines for Managing and Securing Mobile Devices in the Enterprise.* NIST Special Publication 800-124 Revision 1 (Draft). (Authors: Murugiah Souppaya and Karen Scarfone). Gaithersburg, MD. Retrieved from http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf.

National Science Foundation (NSF). February 2011. *FY2012 Budget Request to Congress.* Retrieved from: http://www.nsf.gov/about/budget/fy2012/pdf/fy2012_rollup.pdf.

Networking and Information Technology Research and Development (NITRD). 2010. *Cybersecurity Game-change Research & Development Recommendations*. Arlington, VA: NITRD. Retrieved from: http://cybersecurity.nitrd.gov/page/federal-cybersecurity-1.

North American Electric Reliability Corporation (NERC). 2011. *Critical Cyber Asset Identification* (CIP-002-004). Atlanta, GA: NERC. Retrieved from: http://www.nerc.com/files/CIP-002-4.pdf.

O'Connor, Alan and Ross Loomis. December 2010. *2010 Economic Analysis of Role-Based Access Control*. Report prepared for NIST Program Office. Retrieved from http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf.

Office of the Law Revision Counsel. 2011. "Chapter 35—Coordination of Federal Information Policy." Retrieved from: http://uscode.house.gov/download/pls/44C35.txt.

Office of the Secretary of Defense (OSD). *Office of the Secretary of Defense.* Retrieved from http://www.defense.gov/osd/.

Payment Card Industry Security Standards Council (PCI-SSC). 2011. *PCI SSC Data Security Standards Overview*. Wakefield, MA: PCI-SSC. Retrieved from: https://www.pcisecuritystandards.org/security_standards/index.php.

Payne, S.C. 2006. “A Guide to Security Metrics.” Bethesda, MD: SANS Institute. Retrieved from: http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55.

Perlroth, Nicole. September 30, 2012. “Attacks on 6 Banks Frustrate Customers.” *New York Times.* Retrieved from http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html.

Pisano, Gary P. and Willy C. Shih, July 2009. “Restoring American competitiveness,” Harvard Business Review.

Ponemon Institute. 2012. *The Human Factor in Data Protection*. Traverse City, MI: Ponemon Institute. Retrieved from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf.

Porter, Thomas. July 12, 2012. “The fallacy of remote wiping.” *ZDNet*. Retrieved from http://www.zdnet.com/the-fallacy-of-remote-wiping-7000000611/.

PricewaterhouseCoopers. 2011. *2012 Global State of Information Security Survey*. New York, NY: PricewaterhouseCoopers. Retrieved from: http://www.pwc.com/gx/en/information-security-survey/giss.jhtml.

Raywood, D. 2011. “The Impact of the RSA Token Data Breach Is Still Undetermined.” *SC Magazine*. Retrieved from: http://www.scmagazineuk.com/the-impact-of-the-rsa-token-data-breach-is-still-undetermined/article/198935/.

Richardson, R. 2011. *CSI Computer Crime and Security Survey*. New York, NY: Computer Security Institute.

Romer, Paul M. May 1987. “Growth Based on Increasing Returns Due to Specialization.” The American Economic Review. Papers and Proceedings of the Ninety-Ninth Annual Meeting of the American Economic Association. Vol. 77, No. 2, pp. 56-62.

Rowe, Brent, Michael Halpern, and Tony Lentz. 2012. “Is a Public Health Framework the Cure for Cyber Security?” *CrossTalk*. Retrieved from http://www.crosstalkonline.org/storage/issue-archives/2012/201211/201211-0-Issue.pdf.

Rowe, B.R., D.W. Wood, A.N. Link, and D.A. Simoni. July 2010. *Economic Impact Assessment of NIST’s Text REtrieval Conference (TREC) Program*. Report for NIST. Retrieved from http://trec.nist.gov/pubs/2010.economic.impact.pdf.

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

SANS Institute. 2005. "An Overview of 802.11 Wireless Network Security Standards & Mechanisms." Bethesda, MD: SANS Institute. Retrieved from: http://www.sans.org/reading_room/whitepapers/ wireless/overview-80211-wireless-network-security-standards-mechanisms_1530.

Schneier, Bruce. April 27, 2012. Attack Mitigation. Schneier on Security—A Blog Covering Security and Security Technology. Available at: http://www.schneier.com/blog/archives/2012/04/attack_mitigati.html.

Securities and Exchange Commission, Office of Economic Analysis. 2009. *Study of the Sarbanes-Oxley Act of 2002 Section 404 Internal Control over Financial Reporting Requirements*. Retrieved from: http://www.sec.gov/news/studies/2009/sox-404_study.pdf.

Stoneburner, G., A. Goguen, and A. Feringa. 2002. *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*. Special Publication 800-30. Gaithersburg, MD: NIST. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Tassey, G. 2007. *The Technology Imperative*. Cheltenham, UK: Edward Elgar Publishing.

Tassey, G. June 2008. *Globalization of Technology-Based Growth: The Policy Imperative*. Retrieved from: http://www.nist.gov/director/planning/upload/tassey_jtt_2008.pdf.

The Cooperative Association for Internet Data Analysis. May 2011. *Promotion of Data Sharing*. Retrieved from: http://www.caida.org/data/sharing/.

Treasury Inspector General for Tax Administration (TIGTA). (2012). *Billions of Dollars in Identity-Theft-Related Tax Refund Fraud Go Undetected.* Retrieved from http://www.treasury.gov/tigta/press/press_tigta-2012-36.htm.

U.S. Census Bureau. 2007a. *2007 Economic Census. Table 3. Selected Statistics by Sector*. Washington, DC: Census Bureau.

U.S. Census Bureau. 2007b. *Geographic Area Series: Economy-Wide Key Statistics*. Washington, DC: Census Bureau.

U.S. Department of Commerce. 2011. *Cybersecurity, Innovation, and the Internet Economy*.

U.S. Department of Energy. February 2011. *Congressional Budget Request.* Retrieved from: http://www.cfo.doe.gov/budget/12budget/Content/Volume3.pdf.

U.S. Department of Energy. February 2012. *Congressional Budget Request.* Budget Highlight. Office of Chief Financial Officer. Retrieved from: http://www.cfo.doe.gov/budget/12budget/Content/FY2012Highlights.pdf.

U.S. Department of Homeland Security (DHS). 2009. *A Roadmap for Cybersecurity Research.* Retrieved from: http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf.

U.S. Department of Homeland Security (DHS). 2011a. *FY2012 Budget in Brief.* Retrieved from: http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf.

U.S. Department of Homeland Security (DHS). 2011b. *Safeguard and Secure Cyberspace*. Retrieved from: http://www.dhs.gov/xabout/gc_1240609042614.shtm.

Department of Homeland Security (DHS). 2011c. *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*. Retrieved from http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

U.S. Department of Justice (DOJ), Bureau of Justice Statistics (BJS). 2008. *Cybercrime against Businesses, 2005.* Retrieved from: http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf.

U.S. Department of the Navy. 2011. *FY2012 Budget Estimates Budget Data Book.* Office of Budget. Retrieved from: http://www.finance.hq.navy.mil/FMB/12pres/databook/FY12_Data_Book.pdf.

US-CERT. n.d. *Analytical Tools and Programs.* Available from: http://www.us-cert.gov/federal/analytical.html.

Vogel, V. September 2010. *Glossary*. Internet2. Retrieved from: https://wiki.internet2.edu/confluence/display/itsg2/Glossary.

Water Information Sharing and Analysis Center. n.d. WaterISAC pro member portal. Retrieved from: https://portal.waterisac.org/web/.

Wheatman, V. 2010. *2010 Update: What Organizations Are Spending on IT Security*. Stamford, CT: Gartner Report.

White House. 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Retrieved from: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

White House. 2011a. *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*. Retrieved from: http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

White House. 2011b. *Fact Sheet: Cybersecurity Legislative Proposal*. Retrieved from: http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

Whitney, L. 2011. "RSA to replace SecurID tokens following breaches." Retrieved from: http://news.cnet.com/8301-1009_3-20069632-83/rsa-to-replace-securid-tokens-following-breaches/.

GLOSSARY

Access control: the policies, models, and specifications defining which users have access to which resources at specific times.

Availability: a reasonable assurance that information will be available and free from unexpected disruption.

Avoidance: see Proactive IT Security.

Avoidance cost: the costs of carrying out proactive IT security activities, with the aim of avoiding cyber security attacks.

Best practice: a method or process that is accepted by a significant portion of the industry as the best possible method or process.

Botnet: a group of compromised computers acting in unison to carry out Denial-of-Service (DoS) attacks against a host.

Capital (IT security): hardware and software assets that are used to defend against cyber attacks.

Cloud computing: a model of computing that organizes a set of shared IT resources that can store data or provide services to various subscribers, sometimes enabling subscribers to specify the particular environment in which data or services are being hosted or offered.

Compliance: activities relating to the fulfillment of IT security requirements specified in legislation such as HIPAA or industry standards such as PCI DSS.

Compromise: the loss of a strong guarantee of the security of a resource or data.

Confidentiality: a reasonable assurance that information is not accessed or seen by unauthorized users.

Cyber crime: the use of information technology resources to carry out criminal activities.

Cyber security: the protection from outside intrusion of information technology assets that are connected either to each other through an internal network or to the Internet.

Cyber security attack: an exploitation of a vulnerability in an attempt to gain unlawful access to data or resources.

Cyber security breach: a type of security incident in which the confidentiality or integrity of protected data or a network/system is compromised.

Cyber security cost/loss: harm caused by an executed threat (e.g., theft of personal information or disruption of service or functionality).

Cyber security downtime: the time during which one or more employees are inactive or unproductive due to a disruption of IT resources as a result of a security incident or breach.

Cyber security effectiveness: the capability of an organization in preventing IT security breaches.

Cyber security incident: an attempted or successful compromise of a network/system that may result in loss of network/system integrity.

Cyber security labor: labor effort toward protection against cyber attack.

Cyber security services: activities carried out by third parties (such as vendors, consultants, and contractors) toward the protection of an organization against cyber attacks.

Cyber security technical infrastructure: protocols, data, tools, measures, standards, and technology platforms that assist organizations in protecting their information technology assets**.**

Cyber threat: a vulnerability to or manifestation of particular types of cyber attacks.

Denial-of-service (DoS) attack: an attack aimed at overloading an organization’s server to the point at which the server cannot process legitimate requests from regular users.

Distributed denial-of-service (DDoS) attack: a denial-of-service attack involving several attacks at once coming from many (often thousands) of hosts, making it extremely difficult to cut off the source of the attacks.

Externality: the benefits of performing an activity that are received by entities other than those partaking in the activity.

Gap: in the realm of information technology, a gap is an area in which an organization’s technology, standard, or protocol either does not meet its requirements or is inefficient given newer options; in this report, a gap is an area in which a generic technology or infratechnology is needed to address vulnerabilities (e.g., usable security, enterprise-level metrics).

Generic technology: a laboratory proof of concept derived from basic science. Generic technologies have no specific market applications as stand-alone technologies; rather, they represent a potential trajectory toward a new market application that competing firms draw on in pursuit of innovation.

Identity authentication: verifying the credentials of users attempting to access secure resources and establishing an identity to go along with the user.

Industry association (also called industry consortium): an association of organizations with a common industry, interest, or function, in which either a single body or member organizations provide research, products, or services for the common use of the members or the public.

Industry consortium: see industry association.

Information Sharing and Analysis Center (ISAC): an organization dedicated to the collection, analysis, and distribution of information regarding cyber security threats, attacks, and vulnerabilities; generally, member organizations report threats, attacks, or vulnerabilities, and critical information is passed back to member organizations.

Information technology assets: all of the hardware and software that an organization uses for the storage, operation, and protection of information.

Infrastructure: a foundation for a society or organization supporting its primary function; cyber security infrastructure refers to the foundation technology, standards, and protocols required for an organization to keep its information secure.

Infratechnology: tools that support a variety of infrastructure functions and promote the efficiency of processes, such as research and product development, within an organization.

Insider threat: a cyber threat from one or more people within an organization with access to resources that outside attackers do not have; insiders include employees, vendors, contractors, consultants, and other users with privileged access to resources within an organization's perimeter.

Integrity: a reasonable assurance that information has not been tampered with or corrupted by unauthorized users.

Intrusion detection and prevention system: a tool that monitors networks and other resources for unauthorized access, typically alerting or carrying out preventative action automatically upon discovering an intrusion.

IT intensity: the percentage of an organization's budget dedicated to information technology resources.

Malware: programs that compromise a system by collecting private data or restricting the user's control over certain system resources.

Man-in-the-middle attack: an attack carried out through the interception of a signal from a mobile device in order to steal data or credentials granting access to protected resources.

Marginal cost: the cost of a one-unit or incremental increase in an activity.

Marginal private benefit: the benefit of a one-unit or incremental increase in an activity that is received only by the entity taking part in the activity (i.e., not including external benefits).

Mitigation: see reactive IT security.

Mitigation costs: the costs of reacting to a cyber security attack and minimizing its repercussions.

Mobile platform: the operating system on which a mobile device's software runs (e.g., Windows Mobile, iOS, Android).

Network intrusion: gaining unauthorized access to an organization’s network.

Outsider threat: a cyber threat from one or more entities beyond an organization’s cyber security perimeter.

Payment Card Industry Data Security Standard (PCI DSS): a security standard with a number of rules for organizations that handle payment card data, with the goal of protecting customer data and transactions; this standard is mandated for organizations that wish to accept credit and debit cards.

Personally Identifiable Information (PII): information that can be used to identify an individual (e.g., name, social security number, license number).

Phishing: the practice of pretending to represent a website or organization in order to collect sensitive data or access credentials from unwitting victims.

Physical security: protection of physical access to a building and its resources.

Private cloud: a cloud service environment that is dedicated to only one client, ensuring that resources are not shared among multiple entities.

Proactive IT security (also called avoidance): activities carried out for the purpose of preventing potential/anticipated cyber security attacks and protecting from existing cyber security threats.

Proof of concept: a representation of an idea with the purpose of showing its commercial viability.

Proprietary technologies: processes and products that firms develop on their own for either internal use or restricted external use. With respect to infrastructure, proprietary technologies are methods and tools firms develop to help meet strategic objectives or support the development or products and services.

Protocol: a set of rules or conventions governing how data should be exchanged.

Public cloud: a cloud environment in which multiple subscribers share the same resources.

Reactive IT security (also called mitigation): activities carried out in responding to a cyber security attack with the goal of mitigating the negative consequences of an attack.

Resource: an information technology asset such as a network router or server that can be used to access stored data.

Role-Based Access Control (RBAC): an access control model that assigns access to users based on a list of roles to which users can be assigned.

Security metrics: quantitative or qualitative information about IT security threats, attacks, countermeasures, and IT security resources with regard to the fulfillment of cyber security goals.

Shared threat data: data about threats and/or attacks that are collected and stored by one or more key organizations for distribution to or access from participating organizations.

Social engineering: stealing data or gaining unauthorized access to information technology resources by deception rather than electronic intrusion.

Software as a Service (SaaS): a cloud model in which software is offered virtually (i.e., the software and data are stored remotely) and is generally accessed by a user over the web.

Software exploitation: taking advantage of faulty software, allowing external users to bypass authentication and access protections.

Spyware: see malware.

Stuxnet: a malicious computer program, or worm, that began propagating in 2009, targeting industrial software; possibly considered the most sophisticated worm ever deployed, Stuxnet was believed to be an attempt to sabotage the Iranian nuclear program.

Technical specification: a plan outlining the proposed characteristics of a technology product.

Technical standard: a set of rules or guidelines for products or processes, specifying “the definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength.”[85]

Technical infrastructure: physical assets such as servers, desktops, cabling, and software systems that allow an organization to conduct operations electronically.

Technology platform (also called generic technology): a high-level prototype representing a new technology without defining a commercial application; early-stage research that precedes a proof of concept.

Test bed: an environment for testing concepts, processes, and products.

Threat monitoring: the collection and analysis of qualitative or quantitative information regarding direct threats to an organization or potential threats existing in cyber space.

United States Computer Emergency Readiness Team (US-CERT): an entity within the Department of Homeland Security’s National Cyber Security Division, tasked with improving the nation’s cyber security by coordinating the sharing of threat data and managing cyber security risks.

Virtualization: the creation of a virtual computing environment normally stored on hardware.

[85] http://standards.gov/standards.cfm.

Virus: a program, bundled with a legitimate program, which is designed to replicate itself and make its way onto an unsuspecting computer, where it may carry out various attacks on the computer's data, operating system, or hardware.

Vulnerability: a security weakness (e.g., inadequate software quality, end-user insecurity).

Worm: a stand-alone program designed to replicate itself and make its way onto a computer or network, where it will carry out some kind of damage.

APPENDIX A:
SURVEY INSTRUMENT

A.1 Economic Analysis of U.S. Technology-Based Cyber Security Infrastructure Gaps

The purpose of this study is to identify areas for improving the U.S. technology-based cyber security infrastructure (e.g., standards, standard policies and procedures, data, public-private partnerships for standardization and precompetitive technology development, and best practices) and to quantify the associated economic benefits. Below are a number of background questions that will allow us to use your survey responses appropriately, based on your role, industry and the size of your organization. These background questions are followed by a set of specific questions about your current cyber security activities and processes and the cost savings which your organization may see as a result of specific improvements in the cyber security infrastructure.

Your participation will help to ensure that new investments in the cyber security infrastructure (by both public agencies and private sector organizations) will be focused on areas that will have the greatest economic benefit to organizations like yours.

A.2 About Your Organization

Please characterize your organization's industry and size. Your responses to the following questions will only be used to aggregate with those of other organizations.

What is your title? ________________________

What industry are you in?

Mining, Quarrying, and Oil and Gas Extraction

Utilities

Construction

Manufacturing

Wholesale Trade

Retail Trade

Transportation and Warehousing

Information

Finance and Insurance

Real Estate and Rental and Leasing

Professional, Scientific, and Technical Services

Management of Companies and Enterprises

Administrative and Support and Waste Management and Remediation Services

Educational Services

Health Care and Social Assistance

Arts, Entertainment, and Recreation

Accommodation and Food Services

Other Services (except Public Administration)

Public Administration

Where are you located (CITY, STATE)? ____________________

What was the approximate annual revenue or funding for your organization in 2010? Your best approximation will suffice.

$0–9 million

$10–49 million

$50–99 million

$100–249 million

$250–499 million

$500–999 million

$1,000 million or more

Approximately how many people were employed by your organization in 2010?

0–99

100–249

250–499

500–999

1,000–4,999

5,000–9,999

10,000–49,999

50,000–99,999

100,000 or more

Do you work on IT security for your entire organization?

___ Yes

___ No

6a. If No, for what percentage of your organization’s IT security are you involved?
______ %

As a percentage of your organization’s annual revenue, approximately what size is your organization’s Information Technology budget? (circle one of the ranges below)

1–3%   4–6%   7–9%   10–14%   15–19%   20–30%   >30%

What percentage of your organization’s IT budget do you estimate was allocated specifically for IT security in 2010?

1–3%   4–6%   7–9%   10–14%   15–19%   20–30%   >30%

Consider the resources allocated to your organization’s IT security operations. Please estimate how your organization allocated, in percentage terms, its IT security budget among the following four categories of IT security resources in 2010 *(Note: the total should equal 100%)*:

Labor (full-time, part-time, temporary, and contract employees):________ %
Capital (investment in software and hardware): ________ %
Services (vendors): ________ %
Other (please describe:____________________________) ________ %
100%

Approximately how many IT security employees, measured in terms of Full-Time Equivalent (FTE) employees, were working at your company in 2010? *(Note: as an example, if you had one employee spending 100% time on IT security and two part-time employees spending 50% time on IT security, you would have a total of 2 FTEs)*

________ FTEs

Please review the following definitions before answering the next question:

Proactive investments: IT security spending on labor, capital, or services to help avoid incidents and breaches can be characterized as being *proactive*.

Reactive investments: IT security spending made in response to incidents (e.g., DDoS attacks, viruses, worms, malware, etc.) and breaches (e.g., lost/stolen/altered data) can be characterized as being *reactive*.

Based on the definitions above of proactive and reactive investments, please indicate the degree to which your organization’s spending is more proactive or reactive using the sliding scale below.

Reactive   **Proactive**

As far as you are aware, did your organization participate in any industry consortia (e.g., serving on committees) or work on internal R&D projects specific to IT security standardization in 2010?

Place an x where applicable

Yes___ No___

12a. If yes, approximately how many person-hours did your organization expend in that year for these activities?
______ hours

Specific IT Security Questions

Please review the following definitions before answering the next question:

IT Security Incident: An *incident* is defined as an attempted or successful compromise of a network/system that may result in loss of network/system integrity (e.g., a network is attacked by a DDoS attack, worm, virus. or other malware).

IT Security Breach: A *breach* is defined as a type of security *incident* in which the confidentiality or integrity of protected data or a network/system is compromised (e.g., data is stolen from a server).

Based on the definitions above, approximately how many IT security incidents did your organization observe **in 2010**?

____

13a. What percentage of IT security incidents resulted in IT security breaches?
______ %

Below is a list of IT security activities and processes to which many organizations allocate their IT security budget. Please estimate the percentage of your IT security budget which you allocated to the following activities and processes **in 2010** *(NOTE: Please use the "Other" category for all activities and processes not listed in the table, such as authorization and administrative/management activities. The percentages should add to 100%).*

Activity/Process	% of 2010 IT Security Budget
Responding to employee loss of physical equipment and electronic media	____%
Educating employees about IT security best practices	____%
Identifying potential threats by looking outside your organization (e.g., researching virus signatures)	____%
Gathering/reporting IT security metrics for internal use within the organization (e.g., for presentation to management and for efficiency/effectiveness analysis)	____%
Securing mobile devices	____%
Securing cloud-hosted data, applications, and infrastructure	____%
Manually monitoring and analyzing internal threat data (as opposed to using an automated system/process)	____%
Authenticating all system users	____%
Conducting audits and fulfilling compliance requirements	____%
Other	____%
	100%

How much would you be willing to pay for a 10% improvement in your IT security effectiveness (measured by the number of incidents you deal with each year)?

$ _____________

If your IT security effectiveness improved by 10%, by how much would you be able to decrease your reactive spending (e.g., responding to incidents/breaches such as DDoS attacks, viruses, worms, malware, etc.)? (Note: we recognize that some reactive costs will always be needed to address incidents outside your control, such as certain types of phishing attacks and DDoS attacks)

_________ %

If your IT security budget increased by 10%, how would you spend the additional dollars If you had to allocate them among the activities and processes listed above?

Activity/Process	**What % of Your IT Security Budget Increase Would you Allocate to…**
Responding to employee loss of physical equipment and electronic media	____%
Educating employees about IT security best practices	____%
Identifying potential threats by looking outside your organization (e.g., researching virus signatures)	____%
Gathering/reporting IT security metrics for internal use within the organization (e.g., for presentation to management and for efficiency/effectiveness analysis)	____%
Securing mobile devices	____%
Securing cloud-hosted data, applications, and infrastructure	____%
Manually monitoring and analyzing internal threat data (as opposed to using an automated system/process)	____%
Authenticating all system users	____%
Conducting audits and fulfilling compliance requirements	____%
Other	____%
	100%

We would now like to present you with a series of hypothetical questions to determine the cost of improving each of the activities listed above in terms of effectiveness.

We are interested in whether it would be technically possible for your organization to achieve *on its own* a 10% increase in the IT security effectiveness (e.g., decrease in the number of incidents you have) of a set of activities, if you had a larger IT security budget. For each question below, enter an *x* in the applicable field. If you select *Possible*, enter your estimate of the required budget increase (as a percentage of your current spending in this area) to bring about a 10% increase in effectiveness of each activity. Assume that each of the activities and processes is independent of any other.

On our own, a 10% increase in effectiveness in…

18a. … responding to employee loss of equipment and media is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don’t know ___

18b. … educating employees about IT security best practices is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don’t know ___

18c. … identifying potential threats by looking outside your organization is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don’t know ___

18d. … gathering/reporting IT security metrics for internal use is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don’t know ___

18e. … securing mobile devices is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don’t know ___

18f. … securing cloud-hosted data, applications, and infrastructure is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don’t know ___

18g. … manually monitoring and analyzing internal threat data is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don’t know ___

18h. … authenticating all system users is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don’t know ___

18i. … fulfilling auditing/compliance requirements specifically related to remediation and notification of incidents/breaches
Possible ___ → ___% increase required in budget
Not possible ___
Don’t know ___

If mobile device security could be guaranteed, do you think the number of mobile devices used by your employees would increase? Enter an *x* in the applicable field
___Yes
___ No
___ Don’t know

19a. If Yes, by how much? ______ % increase

If cloud computing security could be guaranteed, do you think your company would use more cloud storage and/or applications on the cloud? Enter an *x* in the applicable field
___Yes
___ No
___ Don’t know

20a. If Yes, by how much?
________ % increase in cloud storage (as a percent of GB used today)
________ % increase in cloud application use (as a percent of traffic used today)

Additional Questions

Now we’re interested in any ideas you may have. What infrastructures, standards, etc. would help your company improve security or reduce IT security-related spending?

____
____
____
____

Is there any additional information you would like to provide?

____

____

____

____

Contact Information

If you are interested in receiving a copy of the final report and/or would be willing to be contacted with additional follow-up questions, please provide your name and contact information and check each appropriate box below.

Name: ____________________

Organization Name: ____________________

Email address:____________________

□ Willing to be contacted with follow up questions

□ Would like to receive copy of final report

NOTE: This questionnaire contains collection of information requirements subject to the Paperwork Reduction Act (PRA). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to penalty for failure to comply with, a collection of information subject to the requirements of the PRA, unless that collection of information displays a currently valid OMB Control Number. The estimated response time for this questionnaire is 20 minutes. The response time includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this estimate or any other aspects of this collection of information, including suggestions for reducing the length of this questionnaire, to the National Institute of Standards and Technology, Attn., Greg Tassey, Gregory.tassey@nist.gov, Mail Stop 1060, 100 Bureau Drive, Gaithersburg, MD 20899, 301-945-2663. The OMB Control No. is 0693-0033, which expires on 10/31/2012.

APPENDIX B:
INTERNATIONAL DATA

Presented are a set of tables created using only data provided by non-US organizations. The tables herein are comparable with data in Section 7, which focused on U.S. companies. Each table created below has a mirror table or figure in Section 7.

Table B-1. Industries Represented by International Survey Respondents

Industry	Number of Respondents	Percentage of Respondents
Finance and Insurance	19	25.68
Information	9	12.16
Manufacturing	3	4.05
Professional, Scientific, and Technical Services	11	14.86
Health Care and Social Assistance	0	0.00
Educational Services	5	6.76
Public Administration	11	14.86
Retail Trade	0	0.00
Utilities	2	2.70
Other Services (except Public Administration)	3	4.05
Wholesale Trade	0	0.00
Services	5	6.76
Mining, Quarrying, and Oil and Gas Extraction	1	1.35
Accommodation and Food Services	0	0.00
Management of Companies and Enterprises	3	4.05
Real Estate and Rental and Leasing	2	2.70
Arts, Entertainment, and Recreation	0	0.00
Construction	0	0.00
Transportation and Warehousing	0	0.00
Administrative and Support and Waste Management and Remediation Services	0	0.00
Total	**74**	

Table B-2. Distribution of International Respondents by 2010 Revenues

Revenue	Number of Respondents	Percentage of Respondents
$0–9 million	19	29.69
$10–49 million	13	20.31
$50–99 million	8	12.50
$100–249 million	4	6.25
$250–499 million	5	7.81
$500–999 million	6	9.38
$1,000 million or more	9	14.06
Total	**64**	

Table B-3. Distribution of International Respondents by Number of Employees

Employees	Number of Respondents	Percentage of Respondents
0–99	19	30.16
100–249	9	14.29
250–499	3	4.76
500–999	5	7.94
1,000–4,999	13	20.63
5,000–9,999	3	4.76
10,000–49,999	7	11.11
50,000–99,999	2	3.17
100,000 or more	2	3.17
Total	**63**	

Table B-4. Employment and Revenue of International Respondents' Organizations (2010)

Field	N	Mean	Median	Total
Revenue	64	$484,138.1	$52,000.0	$30,984,836.5
Employment	61	7,031	375	428,900

Table B-5. Distribution of Cyber Security Spending by Type

Field	n	Mean Percentage of Cyber Security Budget
Labor	51	40.00
Capital (including hardware and software)	51	34.41
Services (including consulting and vendors)	51	23.33
Other	51	2.25

Table B-6. Cyber Security Spending: Proactive vs. Reactive

Field	n	Mean Percentage of Cyber Security Budget
Proactive Spending	55	50.40
Reactive Spending	55	49.60

Table B-7. Willingness to Pay for a 10% Increase in IT Security Effectiveness

Question	n	Mean Percentage of Cyber Security Budget	Mean Amount ($thousand)	Total Amount ($thousand)
As a percent of your IT Security spending, how much would you be willing to pay for a 10% improvement in your IT security effectiveness?	43	14.91%	$95.3	$3,527.8

Table B-8. Allocation of a 10% Increase in Cyber Security Budgets Among CSTI Gap Areas

Gap Area	n	Mean Percentage
Authentication of all system users	39	7.69
Sharing of or access to threat data	39	8.97
Specification and collection of security metrics	39	7.82
Mobile device security	39	11.15
Cloud security	39	12.44
Automated threat detection and prevention	39	6.03
Protection and mitigation from loss of equipment and media	39	8.31
Education about IT security best practices and threat awareness	39	20.28
Standards for meeting auditing and compliance requirements	39	10.26

Table B-9. Estimated Benefits of a 10% Improvement in the CSTI by Gap Area, Surveyed Non-U.S. Organizations Only ($thousand)

Gap Area	Finance and Insurance	Information	Manufacturing	Retail Trade	Health Care and Social Assistance	Utilities	Total (Key Industries)	Total (All Industries)
Education about IT security best practices and threat awareness	586	63	48	0	0	0	697	896
Mobile device security	218	54	65	0	0	0	336	444
Cloud security	205	99	0	0	0	0	304	353
Standards for meeting auditing and compliance requirements	131	63	6	0	0	0	200	349
Authentication of all system users	129	712	26	0	0	0	227	279
Sharing of or access to threat data	86	81	24	0	0	0	191	279
Protection and mitigation from loss of equipment and media	87	71	41	0	0	0	199	275
Specification and collection of security metrics	86	71	24	0	0	0	181	241
Automated threat detection and prevention	86	53	8	0	0	0	147	208
Total	**1,615**	**624**	**241**	**0**	**0**	**0**	**2,481**	**3,324**