Information Technology Industry Council

ITI Recommendation:
Steps to Facilitate More Effective Information Sharing to Improve Cybersecurity
October 2011

Introduction

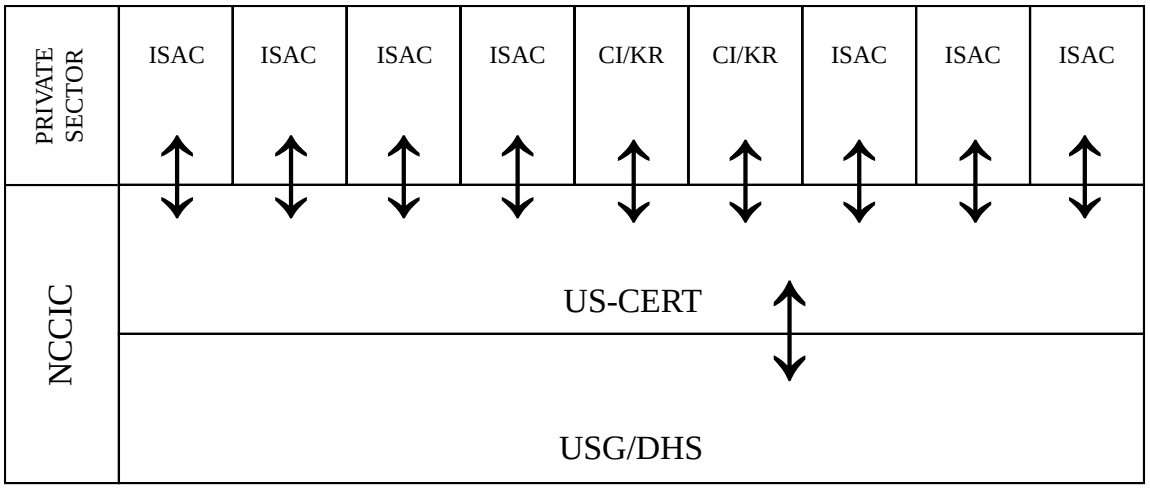
Effective sharing of actionable information among the public and private sectors on cyber threats, vulnerabilities, and incidents is an essential component of improving cybersecurity. Of course, information sharing itself is not the goal, but one of a number of tools to enhance security of information technology (IT) systems. The objective of an effective environment for information sharing is to exchange timely and relevant information that appropriate stakeholders can use to make decisions and take necessary actions to maintain situational awareness, respond to threats and incidents, and manage and mitigate cyber risk. The more actionable and real-time information sharing that we have, the better chance we have in keeping pace with cyber adversaries rather than simply reacting after the fact.

The Information Technology Industry Council (ITI) commends Congress and the Administration for focusing on ways to improve information sharing in the context of cybersecurity. Although many public and private sector entities participate in information sharing activities with varying levels of effectiveness, we concur with the view of many policymakers that information sharing could be improved to better manage cyber risk. Many private sector entities have been long time participants in information sharing activities and strongly support efforts to establish and improve voluntary disclosure protocols with other entities—including the federal government—for threat, vulnerability, or incident information to better protect their own information systems, as well as to assist federal efforts to protect federal systems. Some entities have found information sharing mechanisms useful but there is consensus among ITI members that gaps exist and general guidelines on "how, what, when, and to whom" for sharing information remain unclear. Certain factors, including a lack of mechanisms that support a useful information sharing and analysis partnership, valid fear of legal repercussions, concerns about security of data once shared, and a lack of information sharing protocols and agreements appropriate to each industry sector, preclude many private-sector entities from disclosing actionable information.

ITI is pleased to offer the following recommendations to continue the dialogue with policymakers on how to address the important issues surrounding cybersecurity information sharing. First, we should improve upon existing information-sharing organizations before determining whether new structures are necessary. Our other recommendations focus on two discrete but related areas: improving information-sharing mechanisms and processes, and providing sufficient liability protection. Both of these must be addressed in tandem. Even with improved information sharing mechanisms, unresolved liability concerns could preclude their use by private-sector entities. At the same time, improved liability protection will have little demonstrable impact if weak mechanisms and processes fail to encourage the sharing of actionable information.

Recommendation #1: Improve Upon Existing Structures Before Establishing New Ones

Over the past decade, dozens of organizations and structures have been established to facilitate cybersecurity information sharing among private entities and between the private and public sectors. Some key examples include the Information Sharing and Analysis Centers (ISACs), the U.S. Computer Emergency Readiness Team (US-CERT), and the National Cybersecurity and Communications Integration Center (NCCIC).[1] These and other organizations represent nearly all sectors of the economy as well as federal, state, and local governments. A principal characteristic of these bodies is their diversity. Generally speaking, they have formed to best meet the needs of their particular members. For example, the 16 ISACs represent sectors as diverse as IT, financial services, communications, healthcare, and public transportation and vary greatly in membership, scope, and capabilities. Of course, not all private-sector entities belong to ISACs, but may use other information sharing arrangements, such as direct engagement or through existing sector organizations not specifically designated as ISACs. The US-CERT is the government's conduit to the ISACs for cybersecurity matters, acting as a 24/7 single point of contact between DHS and the critical infrastructure/key resource (CIKR) community for cyberspace analysis, warning, information sharing, and incident response and recovery. The NCCIC is a 24/7 watch-and-warning center that is the locus of DHS-led inter-agency cybersecurity work. It provides an integrated response to cyber threats against government networks, and coordinates any requested government aid and response to cyber incidents on private industry networks, such as industrial control systems. Many of these organizations and others in turn are part of the larger information-sharing framework under the National Infrastructure Protection Plan (NIPP).



While much work remains to be done, notable progress has been made in populating and effectively using these information-sharing organizations to manage and mitigate

[1] DHS's 2009 National Infrastructure Protection Plan (NIPP) "Chapter 4: Organizing and Partnering for CIKR Protection" describes these and dozens of other information sharing nodes used by DHS and other federal agencies, the law enforcement community, state and local governments, and the private sector.

cybersecurity risks. Some examples are below.

- *IT-ISAC:* In April 2009, the IT-ISAC responded to the Conficker worm through various means, including issuing bulletins, hosting calls with members across the critical infrastructure sectors, and sharing information with other security partners. In December 2010, the IT-ISAC provided analysis of a series of cyber incidents known as "Operation Payback" during the WikiLeaks controversy.
- *Financial Services (FS) ISAC:* The FS-ISAC reaches more than 20,000 sector participants daily and promotes information sharing between the public and private sectors. The FS-ISAC allows its members to receive threat and vulnerability information immediately, communicate within a secure portal to share vulnerability assessments and other information anonymously, and access new data feeds of threat and vulnerability information. The FS-ISAC has implemented a crisis communications system to notify its members of emergencies in minutes.

Despite the long-standing existence, track record, and trust gained by these and other entities within their sectors, there is often a desire to establish new organizations to address the ongoing challenges we face in this space. While new organizations may present an attractive solution, we are concerned that they could unnecessarily duplicate the myriad of activities underway, undermine significant investments made to date, and strain the limited resources (both money and staffing) that the private sector can devote to information sharing organizations. Further, the importance of personal and organizational trust for information sharing—company to company, company to government, company to client—cannot be overstated. Such trust takes years to establish. The ability to leverage the significant trust relationships that have been established over the years that enable much of the information flows among all actors in current organizations and the internal processes they have put into place to ensure that their trust models are sustainable and reliable must not be minimized or put at risk. Finally, many existing organizations have amassed innumerable "lessons learned" and best practices that must continue to guide our efforts, and developed ongoing working relationships across sectors. For these reasons, any initiative to create new information sharing organizations or arrangements must be rationalized in the context of the existing structures that industry and government have invested in for years.

Thus, the most effective path to improving information sharing and shoring up our cyber posture is to leverage these current organizations and evolve them into more effective partnerships for true sharing. The government should provide a single point of entry to work in consultation with relevant stakeholders, including the private sector and sector-specific agencies (SSAs, such as the Department of Energy or others in charge of regulated sectors), to develop mutually agreed upon information sharing objectives and jointly identify and implement ideas for improvement. This approach would be consistent with ITI's "Cybersecurity Principle 1," which states that efforts to improve cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments. To support that Principle, ITI proposes that policymakers should:

- Recognize that many public-private partnerships have been in existence for a decade or more and have helped to establish a significant amount of trust among actors. They also benefit from significant industry resource commitments;
- Leverage and build upon existing partnerships and efforts to the fullest extent possible, including those that work to advance critical infrastructure protection; and
- Determine which public-private partnership(s) may be addressing issues about which policymakers are concerned, and leverage them as appropriate before proposing something new (particularly before proposing any new structure at odds with such partnerships).[2]

The sections below provide specific ideas on how existing organizations, processes, or mechanisms can be improved.

Recommendation #2: Improve Existing Information Sharing Mechanisms and Processes

Issue: The 2009 NIPP states, "The effective implementation of the NIPP is predicated on active participation by government and private sector partners in meaningful, multidirectional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to CIKR and participate in ongoing multidirectional information flow, their ability to assess risks, make prudent security investments, and develop appropriate resiliency strategies is substantially enhanced. Similarly, when the government is provided with an understanding of private sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly."[3]

Unfortunately, today the "comprehensive picture of threats or hazards" upon which decisions should be made is not as specific, actionable, or timely as is needed. Nor is the bidirectional information flow as effective as it could be. Improvement can be made in terms of information synthesis and dissemination to the right people in a timely manner with appropriate classification/declassification so that the CIKR owners and operators can use it. CIKR owners and operators need accurate and timely incident and threat-related information to effectively manage risk, enable post-event response and recovery, and make decisions regarding protection strategies, partnerships, mitigation plans, security measures, and investments for addressing risk.

Weaknesses identified in the current system include the following:

- Information shared by DHS and other federal government agencies often is too generic or outdated to be of use. The government should be providing unique intelligence based on its unique insights.
- At the same time, information shared by DHS also often is over-classified to the

[2] See The IT Industry's Cybersecurity Principles for Industry and Government, Principle 1: "Efforts to improve cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments"—What More Can Policymakers Do? p. 11, found at www.itic.org.
[3] See 2009 NIPP, p. 56.

extent that it cannot be shared with the private sector. In addition, information used during law enforcement investigations sometimes is made "law enforcement sensitive," restricting its sharing or further use.

- DHS sometimes does not share information with ISACs out of concern that, because some ISACs are supported by membership fees, providing information to such entities is "unfair" to non-members. DHS should share information with all relevant organizations, including ISACs.
- Efforts to place cleared industry personnel on the floor of the NCCIC have been stymied by legal issues within DHS. For example, the IT-ISAC placed an individual on the floor for several months, but that person was not allowed to remain due to changing DHS legal requirements. In addition, operational constraints such as reach-back to IT-ISAC networks and classification issues stymied the effectiveness and reduced the value of the participation. It is interesting to note that IT-ISAC representatives are able to deploy to the DHS Office of Infrastructure Protection's National Infrastructure Coordination Center (NICC) for collaboration on national response to physical incidents, but are not afforded the same operational interaction with the NCCIC, also operated by DHS.

Solution: Under the NIPP, DHS and the SSAs are expected to work with the private sector to measure the efficacy of the information sharing processes and identify areas in which new mechanisms or supporting technologies are needed.[4] Thus, Congress should direct DHS to do the following:

- Work with the IT sector to overcome unique legal barriers to information sharing by creating flexible legal frameworks.
- Share information with ISACs, Sector Coordinating Councils (SCCs), and other relevant bodies in ways appropriate to their roles, capabilities, and trust models. Also, share information directly/bilaterally with CIKR owners and operators as appropriate.
- To address problems of information flow, establish a temporary public-private entity under the NIPP framework that consists of all relevant SSAs and private-sector stakeholders that will, over a finite time period (such as 90-120 days), develop a plan to meet the following objectives:
    - Define a clear outcome we seek to achieve;
    - Define with whom certain information should be shared;
    - Define key indicators needed (specifically the technical aspects) to be identified and provided in alerts, warnings, and notifications;
    - Define what type of labeling is needed for data (e.g. sensitive, for official use only, general) and in what cases each label should be used;
    - Define how information should be anonymized—for example, DHS should determine how to better use existing structures to do so, such as the Protected Critical Infrastructure Information (PCII) Program of the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B of the law that created DHS); and
    - Define how information packaged as above can/cannot and will/will not

[4] See 2009 NIPP, p. 61.

be used and shared by both public and private sector organizations.

- Establish regularized processes for communicating actionable threat and other cybersecurity related information in ways usable by ISACs and other stakeholders, and share such information in accordance with jointly established protocols and appropriate security controls.
- Declassify information as much as possible.
- For information that must remain classified, make effective use of industry representatives who hold security clearances, and expedite necessary clearances for designated points of contact in industry where such clearances are needed.
- Provide baseline funding for the core functions of all ISACs (such as funding for DHS support personnel, as is currently done to support the Sector Coordinating Councils). ISACs could then choose to self-fund any additional capabilities.
- Encourage appropriate private-sector entities to join the ISACs or SCCs. This could be done as part of a broader cybersecurity campaign and/or through SSAs and other industry-specific entities. Improvements in actionable information sharing from government will in fact serve as an incentive for greater industry participation in such entities.
- Designate one point of contact within the Department, such as an entity within the National Protection and Programs Directorate (NPPD), which is ultimately responsible for overseeing and coordinating DHS's information sharing activities.
- Issue a report to Congress on a regular basis describing the efficacy of information sharing. Such a report should be based on input and analysis from industry's perspective, not just from DHS. It should focus not on the quantity of information exchanged (such as number of bulletins issued) but on the quality—namely the value of actionable information. The report should cover multidirectional information sharing including the value of information DHS receives from the private sector.

Congress should mandate that DHS, SSAs, and private sector stakeholders under the NIPP framework jointly report to Congress annually the progress on the tasks above.

Finally, the government should address intra-governmental information sharing issues and challenges.

Recommendation #3: Address Liability Concerns Related to Information Sharing[5]

Issue: The sooner actionable information about cybersecurity threats is shared among organizations, the faster it can be used to help protect information systems and networks including government systems, critical infrastructure entities, and the general public. Even the most security-conscientious businesses, however, may hesitate to bring forward

[5] Liability related to voluntary sharing of information related to cybersecurity threats and incidents is just one type of liability relief that needs to be addressed to improve cybersecurity. Other liability concerns arise from actions taken by the private sector to address cyber incidents resulting from government-declared cyber emergencies, etc.

that information broadly to government or to their peers in a timely way. A company may fear that to associate itself with a cyber threat is to court potentially crushing liability when it, too, is being victimized. In fact, liability concerns remain a major impediment to greater information sharing by private entities of cybersecurity threats.

More specifically, there are two main categories of liability concerns related to voluntary disclosure of information regarding cybersecurity threats, vulnerabilities, and incidents:

1) *Harm from accidental disclosure of the information:* In this case, information that is voluntarily shared with the government or another private-sector entity is lost, disclosed, exploited, or otherwise misused. The private-sector entity providing the information voluntarily had done so in the belief that the information would be in a safe place and treated appropriately.
2) *Harm from exploitation of a reported vulnerability:* In this case, government prosecutors, law enforcement agencies, or civil attorneys use information that was voluntarily disclosed by a private-sector entity for the purposes of protecting cyberspace as the basis for establishing a violation of civil or criminal law. Limiting liability in this case would not aim to insulate the private-sector entity from any legal proceedings, but would clarify that the information it shared cannot be the proof used.

Solution: Treating organizations as trusted partners will be an incentive for them to be more proactive in stepping forward in the interests of their customers, employees, shareholders, and the national interest. To encourage organizations in possession of actionable threat information to come forward, Congress should introduce proposals to clearly extend liability protection to both the disclosure of the information and to the resulting impact from exploitation of a reported vulnerability.

Sections 245 and 246 of the Administration's May 2011 legislative proposal took steps to address liability concerns by introducing proposals to limit liability when such information is voluntarily shared. However, as ITI noted in our comments on that proposal, we are concerned that these proposed liability protections contain some ambiguities that may not adequately incentivize the level of information sharing desired and needed for purposes of strong cybersecurity. Specifically, although the language in the White House proposal protects the action of information sharing, it does not expressly address liability in connection with an actual vulnerability or incident. Thus, if a private-sector entity were to notify the federal government of a threat, and that threat became known, the entity would be at risk of legal action (the first concern listed above).

The House Republican Cybersecurity Task Force, in its recently released recommendations, also addressed the issue of liability, expressing the belief "that information sharing within existing structures can be improved through limited safe harbors when private sector entities voluntarily disclose threat, vulnerability or incident information to the federal government or ask for advice or assistance to help increase protections on their own systems." The Task Force further pointed out that such liability protections would additionally need to address concerns about antitrust issues, FOIA exceptions, and a host of other liability-related concerns. ITI looks forward to the

opportunity to help Congress to build on these recommendations and work through the complicated issues in this area.

To address liability concerns, we recommend that Congress introduce language that would:

- **Protect organizations cooperating with law enforcement and other government entities.** Organizations cooperating with a law enforcement body, DHS, or DOD should have a defense against claims for failure to warn when a qualified law enforcement agency formally instructs that no further disclosures be made. This would occur after an appropriate determination by the government that disclosure could reveal law enforcement methods or sources, impede investigations, or impair national security. In support of this recommendation, Sections 245-246 of the Administration's legislative proposal provide that voluntary disclosures to the government will not be the basis for lawsuits. We concur that these disclosures should be off-limits to plaintiffs in suits against organizations who step forward.
- **Ensure that communications disclosed by private entities to the government are subject to appropriate protections.** This is a critical step to allow the private sector to understand not only the risks and liabilities associated with cooperating with the government and receiving information from the government, but also whether and how information that the private sector shares with the government will be used and protected and how it may be moved between and among entities.
- **Leverage the PCII program.** Finally, legislation regarding information sharing should refer to the PCII Program of the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B of the law that created DHS). Section 214 of that Act provides for specific protections for such shared information, including remedies for violations and breaches. The PCII program is now a mature program, with updated implementing rules and usage by multiple sectors. The PCII program also covers liability, and provides for Federal, state, and local government stakeholders to participate, as long as they agree to the requirements. In conjunction with private sector stakeholders, this program can be used more effectively and enhanced as needed.