ICIT - Institute for Critical Infrastructure Technology

April 16, 2015

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit (status pending), non-partisan group of the world's most innovative experts and companies that provide technologies and solutions to support and protect our Nation's critical infrastructures.

Although the U.S. has faced cyber attacks on its critical infrastructure network since the earliest days of the Internet, the recent high profile attacks on Sony, Anthem Blue Cross-Blue Shield, Target, and others have finally made the American public aware of the cyber threat. Somewhat surprisingly, the United States continues to lack a comprehensive strategy to combat cyber attacks. One of the primary hurdles to the development of such a strategy is the lack of threat-information (TI) sharing between the private sector and government. Given that the majority of US infrastructure is controlled by the private sector, establishing a safe way to share information is crucial.

The concept of a TI sharing portal has risen to prominence among lawmakers on Capitol Hill as well as President Obama. As Congress continues to wrestle with myriad complexities stemming from this idea, ICIT believes the following analysis will add value to your efforts.

Industry concerns involving information sharing

Privacy and legal concerns continue to represent a significant roadblock to robust sharing. For instance, there is concern involving the Freedom of Information Act (FOIA) and the security of the data stored by the TI-sharing forums. The threat of a FOIA request by a public interest group or competitor that would compel a company to reveal or compromise proprietary information acts as a disincentive to open sharing.

Any information sharing portals must also take into account the amount of sensitive data being shared with government during the RFP process. Companies will be reticent to engage any process that hinders its ability to successfully compete in the highly competitive RFP system, as well as partner with other companies.

Furthermore, industry faces challenges in vetting sources and dedicating sufficient resources to digest and act on shared data. This allocation of financial resources can prove difficult to allocate and account for through corporate accounting techniques. Moreover, many CIOs of publically traded companies will find spending shareholder revenue on compliance

toward information sharing practices that may be seen in a negative light by the public, to be highly problematic.

The format in which companies are asked to report can also be a concern. Companies, as well as government agencies, produce reports in myriad styles and formats. Undoubtedly, there will be problems with standardization of formats, with some reporting companies failing to meet new formatting requirements, either by choice or because of a lack of capability.

In contrast, industry partners, in a well-meaning effort to be thorough and/or to avoid liability, might overwhelm government officials with massive data-dumps. Technology infrastructure companies simply do not have the analytic and investigative capabilities of a government-run intelligence agency.

Strong liability protection must also be included in any new information-sharing regime. Currently there are multiple initiatives emanating from the House of Representatives. Regardless of whether one of these bills rise to the top or a combination of many efforts proves to win the day, clear language that ensures sharing of cyber information will not be used against a non-Federal entity.

Is a single government-controlled portal the best solution?

A key concern involves relative magnitude. If Congress creates a government-controlled information-sharing portal it should account for the respective budgets and profit margins being pursued by a wide variety of organizations. While large technology organizations can usually absorb new costs associated with mandatory information-sharing requirements, the associated costs can be prohibitive for smaller and medium-sized IT firms.

Currently some of our Nation's Information Security and Analysis Centers (ISAC) share information through a program called Soltra Edge, which operates on the machine-readable language Structured Threat Information eXpression (STIX) and transmitted via the Trusted Automated eXchange of Indicator Information (TAXII) protocol for transporting the information.

Moreover, the Financial Services Information Security and Analysis Center (FS-ISAC) has a Security Automation Working Group that lead to the creation of Project Avalanche, a collaborative effort between DTCC & FS-

ISAC to establish Soltra (www.soltraedge.com). The original funding for this cyber threat intelligence-sharing platform came from a consortium of sixteen banks. This is an example of a successful community that's sharing tactical TI today.

The types of data shared are different due to (i) communities of interest, (ii) perspective, (iii) legal concerns, (iv) to whom the data is going, and (v) the perspective that it has on international customers. There is a need to have sharing across industries to ensure threat vectors used in one industry are sufficiently addressed in other industries. For example, attacks against the financial sector may appear in the retail & healthcare industry.

It remains to be seen how the ISACs will operate under the new ISAO model created by Executive Order (EO) 13691. The Department of Homeland Security (DHS) has tapped Mike Echols, JPMO Director, SECIR, CS&C at DHS as the Implementation Manager for EO 13691. Assuming he can improve upon their success thus far, DHS would be well served to see how this new model operates before implementing yet another organizational paradigm shifts.

In addition, the question of "mandatory" versus "optional" use is an extremely important determination that must be clearly defined in original legislative language. There will clearly be companies that will eagerly cooperate and those that will be apprehensive. Industry must know what penalties, hidden or otherwise, will be brought to bear on companies that choose not to participate, and what incentives will be available to those who opt to engage the new project.

All parties, be it government or industry, will clearly need assurances that the data shared is protected. There have been countless examples of high-profile breaches in government and military agencies as well as respected corporations. The best way to ensure trust is to engage industry partners from the beginning of the process rather than waiting until a breach-event to engage. Working with industry and all relevant stakeholders to build in security protocols from the beginning will go a long way toward cultivating a spirit of cooperation.

Privacy is also a concern for industry as well as many citizens. For instance, the Cybersecurity Information Sharing Act of 2015 (CISA) is also currently being considered on Capitol Hill. We believe this legislation that would increase the government's authority to analyze threat information without the proper balance of privacy concerns for citizens. Many will wonder

how government authorities will handle the personal information shared. Current legislation being discussed offers multiple distinct approaches toward this matter. ICIT believes the most robust possible privacy protocols are adopted in any new information sharing legislation.

However, the Department of Homeland Security, as opposed to the National Security Agency (NSA), should lead any effort toward government controlled information sharing. This is a necessary but not sufficient step toward assuaging privacy fears among US citizens. In addition, the issue how about federal law enforcement will use data collected through information sharing. In the past, we have seen federal agencies use data in ways not envisioned by Congress. We must be sure that if data will be used across multiple federal agencies, this capability must be made clear in legislative language.

There needs to also be additional legislative safeguards focused on civil liberties. Cybersecurity legislation should be designed to increase security by identifying and remediating threats, and not stoke fears of a creep toward a surveillance state that could compromise privacy. The Snowden revelations about generations of NSA-led clandestine data gathering on American citizens has understandably made the Nation's citizenry highly wary of the US Government's ability to 1) protect sensitive data, and 2) avoid overreaching and exceeding their mandate. With so much critical infrastructure data in the hands of the private sector, there is a potential tidal wave sensitive data to be handed to the government. It will take a great deal of assurance to assuage the concern among many that the US is moving inexorably toward a surveillance society.

*Expert research contributed by the following ICIT Fellows:

- William J. Billings (ICIT Fellow - Security Strategist, U.S. Public Sector, HP)
- Stan Wisseman (ICIT Fellow – Security Strategist, Strategic Accounts, HP)
- Cynthia Cullen (ICIT Fellow - Security Strategist, Northeast, HP)
- Chris Schumacher (ICIT Fellow - Sr. Technology Consultant, New Light Technologies)
- Danyetta Fleming (ICIT Fellow – President & Founder, Covenant Security Solutions)
- Daniel Skinner (ICIT Fellow – Chief Product Officer, Watchdox)
- Dan Waddell (ICIT Fellow - Director, Government Affairs, (ISC)2)

ICIT - Institute for Critical Infrastructure Technology

- James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- Morgan P. Muchnick (Senior Director of Legislative Affairs – Institute for Critical Infrastructure Technology)