

INFORMATION SHARING:

If It's Such a Good Thing, Why Isn't Everyone Doing It?

Ira E. Hoffman, Esq.
Of Counsel
Butzel Long

OUR NATIONAL SECURITY RELIES ON OUR ABILITY TO SHARE THE RIGHT INFORMATION, WITH THE RIGHT PEOPLE, AT THE RIGHT TIME.


Our national security relies on our ability to share the right information, with the right people, at the right time.¹

While the high-profile attacks against Target, e-Bay, Home Depot, Nieman Marcus, JPMorgan Chase, Sony Pictures Entertainment, Anthem, the IRS, and OPM have enhanced awareness of the depth and breadth of harm that organized cyber attacks can pose, they are only a very small number of the publicly disclosed attacks perpetrated against entities in the U.S. over the last two years. Indeed, credible sources tend to believe that “hundreds of thousands” of other entities likely suffered similar incidents during the same period,² with one survey asserting that 43% of business firms in the U.S. had discovered a data breach between 2013 and 2014.³ According to the Congressional Research Service (CRS), the consensus view is that the

cyber attacks of the last few years will be eclipsed by “more frequent and more sophisticated” cyber incidents going forward.⁴ What, then, can we do to slow, if not stop, this tide? One answer is to enable and increase information sharing about cyber incidents and successful defensive techniques between private-sector entities and the Federal government.

The idea of information sharing is nothing new. As far back as 1998, President Bill Clinton expressly recognized that our military power and national economy were both increasingly reliant on “cyber-based information systems,” and advocated the voluntary formation by the private sector of an Information Sharing and Analysis Center (ISAC).⁵ Yet it took Congress several years to ask the General Accounting Office (GAO) to survey a number of stakeholders in cyberspace on factors that were deemed critical to information-sharing relationships.⁶

Although the 9/11 attacks cannot be attributed to cyber vulnerabilities, the Homeland Security Act of 2002 not only created the Department of Homeland Security (DHS), but also included the Homeland Security Information Sharing Act, which required Federal agencies to share information about terrorist activities,⁷ and the Critical Infrastructure Information Act of 2002, which encouraged the private sector to voluntarily submit information concerning critical infrastructure and protected systems that was not customarily in the public domain, and directed the Secretary of Homeland Security to establish procedures for protecting such information.⁸



The idea of information sharing is nothing new. As far back as 1998, President Bill Clinton expressly recognized that our military power and national economy were both increasingly reliant on “cyber-based information systems,” and advocated the voluntary formation by the private sector of an Information Sharing and Analysis Center (ISAC).

Unfortunately, the Federal government failed to achieve effective information sharing with stakeholders in the critical infrastructure sector,⁹ and attempts to promote information sharing beyond critical infrastructure sectors by Presidents Bush and Obama in 2008 and 2010, respectively, made only modest progress.¹⁰ In 2011, Congress tried to eliminate obstacles to information sharing relating to cyber attacks in the Cyber Intelligence Sharing and Protection Act (CISPA), but while the bill passed the House it was never acted upon in the Senate.¹¹ Frustrated by lack of progress in Congress, President Obama issued an Executive Order on improving cybersecurity for our critical infrastructure in February 2013, which declared that it is the “policy of the U.S. Government” to increase the “volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities” so that they may better protect themselves against cyber threats. At the same time, the President also directed the National Institute of Standards and Technology (NIST) to create a Cybersecurity Framework to help owners and operators of critical infrastructure assets identify, assess and manage cyber risk.¹²


Since then, NIST has issued not only the Framework, but also a draft Guide to Cyber Threat Information Sharing,¹³ and Congress passed the National Cybersecurity Protection Act of 2014.¹⁴ Although the Act has a broad-sounding name, it has a relatively narrow scope, which consists primarily of establishing a National Cybersecurity and Communications Integration Center in DHS, and specifying that the Center’s functions include acting as an “interface” for sharing information about cyber risks, incidents, analysis, and warnings for Federal and non-Federal entities. Finally, in February 2015, the President issued Executive Order 13691, which expressly encouraged the voluntary formation of Information Sharing and Analysis Organizations (ISAOs) and of an ISAO standards organization.¹⁵

If our national security depends on information sharing, and it is a national priority to share threat information, then why isn’t everyone doing it? There is no definitive answer, but three of the most oft-cited reasons are cost, risk of disclosing proprietary information, and risk of exposure to liability for releasing Personally Identifiable Information (PII).¹⁶



An additional challenge to information sharing is that organizations fear raising antitrust issues, but this concern is unfounded. Specifically, the Department of Justice and the Federal Trade Commission, the enforcement agencies for the antitrust laws, have issued a Joint Statement that makes it clear that they do not believe that antitrust is or should be a roadblock to legitimate cybersecurity information sharing because cyber threat information is typically very technical and “very different from the sharing of competitively sensitive information such as current or future prices and output or business plans.”¹⁷

IF OUR NATIONAL SECURITY DEPENDS ON INFORMATION SHARING, AND IT IS A NATIONAL PRIORITY TO SHARE THREAT INFORMATION, THEN WHY ISN'T EVERYONE DOING IT?

So where does that leave us? Given the history of efforts to promote information sharing, Congress must step up and pass legislation that will provide greater incentives, such as exemption from liability for disclosures made for purposes of information sharing, to private industry, encouraging more active participation in information sharing. Otherwise, the gains from information sharing will grow at a snail's pace, if at all. 

Sources

1. The White House, “National Strategy for Information Sharing and Safeguarding,” at 3 (Dec. 2012), available at https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (emphasis added).
2. See Pricewaterhouse Coopers, Managing Cyber Risks in an Interconnected World, page 7, note 11 (Sept. 30, 2014), available at <http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml>.
3. Ponemon Institute, Is Your Company Ready for a Big Data Breach? page 1 (Sept. 2014), available at <http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf>.
4. CRS, “Cybersecurity and Information Sharing: Legal Challenges and Solutions,” CRS No. R43941, at 2 (Mar. 16, 2015).
5. See The White House, “Presidential Decision Directive 63: Critical Infrastructure Protection,” 1, 13-14 (May 22, 1998), available at <http://fas.org/irp/offdocs/pdd/pdd-63.pdf>.
6. See GAO, “Information Sharing: Practices That Can Benefit Critical Infrastructure Protection,” GAO-02-24 (Oct. 2001). The GAO has since been renamed the Government Accountability Office.
7. Pub. L. No. 107-296, §§ 891-899, 116 Stat. 2252 (2002).
8. Pub. L. No. 107-296, tit. II, §§ 212-221, 116 Stat. 2150 (2002).
9. See, e.g., GAO, “Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors,” GAO-04-780 (July 2004); GAO, “Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities,” at 3 (May 2005); GAO, “Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information,” (Mar. 2006).
10. See Memorandum on Designation and Sharing of Controlled Unclassified Information (CUI), 44 Weekly Comp. Pres. Docs. 673 (May 7, 2008); Exec. Order No. 13556, Controlled Unclassified Information, 75 Fed. Reg. 68,675 (Nov. 9, 2010).
11. H.R. 3523, 112th Cong.
12. Exec. Order No. 13636, “Improving Critical Infrastructure Cybersecurity,” 78 Fed. Reg. 11,739 (Feb. 19, 2013).
13. NIST, Guide to Cyber Threat Information Sharing (Draft), Special Publication 800-150 (Draft) (Oct. 2014).
14. Pub. L. No. 113-282, 128 Stat. 3066 (2014).
15. Exec. Order No. 13,691, “Promoting Private Sector Cybersecurity Information Sharing,” 80 Fed. Reg. 9349 (Feb. 20, 2015).
16. See, e.g., NIST Guide to Cyber Threat Information Sharing (Draft), Special Publication 800-150 (Draft) at 7-8.
17. Dep’t of Justice and FTC: Antitrust Policy Statement on Sharing of Cybersecurity Information, 1, 3 (2014), available at <http://www.justice.gov/sites/default/files/atr/legacy/2014/04/10/305027.pdf>.

About the Author:



Ira E. Hoffman, Esq., is Of Counsel in the Aerospace and Defense Practice Group at Butzel Long, a leading law firm with offices in Washington, D.C., New York and Michigan. He was Co-Chair of CyberMontgomery 2015; and is Co-Chair of the Tech Council of Maryland Cyber Committee, a Fellow of the Cyber Security Forum Initiative (CSFI), an instructor for the Public Contracting Institute (PCI), and a frequent speaker and author of several articles on cybersecurity law and policy. He can be reached at 202-454-2849 or at hoffmani@butzel.com.

