The Heritage Foundation

BACKGROUNDER

No. 2899 | APRIL 1, 2014

Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace

David Inserra and Paul Rosenzweig

Abstract

The Internet can be a powerful engine for growth and freedom, and the United States is taking full advantage of its enormous benefits. Since everything from military systems to smartphones has become linked to the Internet, however, the number of bad actors seeking to attack or steal from those targets has increased dramatically. Hackers compromise, steal, or destroy hundreds of billions of dollars in intellectual property and real money, as well as accessing critical military secrets from the United States, every year. Yet Congress has taken no tangible and effective steps to counter this persistent and growing threat. One effective policy would be the sharing of cybersecurity threat and vulnerability information between the private and public sectors. By sharing information, different entities in the two sectors can be warned about likely attacks or specific problems created in the software. With proper protections, frameworks, and oversight, the United States can—and should—take advantage of this cost-effective and dynamic form of security.

The Internet is a powerful engine for growth and freedom, of which the United States has taken and continues to take full advantage. As everything from military systems to smartphones has become linked to the Internet, however, the number of bad actors seeking to attack or steal from those targets has increased dramatically. Hackers compromise, steal, or destroy hundreds of billions of dollars in intellectual property and real money, as well as accessing critical military secrets from the United States, every year.[1]

While the U.S. government is finally starting to become aware of the problem, Congress has taken no tangible and effective steps

Key Points

- Sharing of cybersecurity threat and vulnerability information between the private and public sectors is important because it alerts companies and agencies to likely attacks or specific problems in the software.
- To make information sharing effective, Congress and the Administration should organize sharing efforts so that they flow rapidly and in both directions between the government and the private sector.
- Enabling sharing requires that the private sector be provided with legal, FOIA, and regulatory protections for sharing information so that companies are not punished or harmed when they share.
- Information sharing should be broad enough to ensure that government agencies have the information they need in order to prevent cybercrime and attacks.
- It is important that information sharing be matched with robust, but not restrictive, oversight to ensure that information is used appropriately.

This paper, in its entirety, can be found at **http://report.heritage.org/bg2899**

Produced by the Douglas and Sarah Allison
Center for Foreign and National Security Policy

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

to counter this persistent and growing threat. It is important that Congress act, but it is more important that it pursue the right policies—policies that will in fact improve cybersecurity efforts. One example of such a policy is the sharing of cybersecurity threat and vulnerability information between the private and public sectors. By sharing information, different entities in the two sectors can be warned about likely attacks or specific problems in the software.

To make information sharing effective, several things are needed. First, Congress and the Administration must do a better job of explaining to the American people what information sharing is and how it works in order to address real privacy concerns and overcome a serious lack of trust in government. Second, since cyber threats and vulnerabilities are constantly changing, information sharing must be organized to flow rapidly and in both directions between the government and the private sector. Third, the private sector must be provided with legal, Freedom of Information Act (FOIA), and regulatory protections for sharing information so that companies are not punished or harmed when they share. Finally, information sharing should be broad enough to ensure that government agencies have the information they need in order to prevent cybercrime and attacks. It is important, however, that such sharing be matched with robust oversight measures to ensure that information is used appropriately.

The Ins and Outs of Information Sharing

The first step in a rational discussion of any policy is to understand what exactly the policy does. In the case of cybersecurity information sharing, data on the latest threats and vulnerabilities are voluntarily shared with a variety of different entities in and out of government. This information is used to prevent further cyber attacks and crimes and, in some cases, crimes and attacks of a non-digital nature.

A major concern with information sharing stems from *who* has access to *what*. Critics worry, for example, that the National Security Agency (NSA) might have access to individuals' e-mail messages. This is a legitimate concern (given recent revelations) but one that can be addressed by looking at the various definitions used to describe what is being shared.

The cybersecurity bills that Congress has thus far considered have had relatively similar definitions of what constitutes "cyber threat intelligence" or "cybersecurity threat indicators"—that is, the kind of information being shared. The definition of cyber threat intelligence used by the Cyber Intelligence Sharing and Protection Act (CISPA) that passed the House in 2013 provides a good example because it is so recent. It described information to be shared as "intelligence … directly pertaining to

i. a vulnerability of a system or network of a government or private entity or utility;

ii. a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

iii. efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility;

iv. efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.[2]

The first clause deals with cyber vulnerabilities in software, hardware, network or firewall configurations, or other systems that can be exploited by hackers if not discovered and repaired by IT professionals. Sometimes these vulnerabilities are relatively well known, while in other cases these vulnerabilities may be completely unknown until a hacker finds and exploits them in what are known as "zero day exploits." Both kinds of vulnerabilities give hackers access to computer systems or networks, with the potential to steal, degrade, or destroy information or

[1] *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property,* National Bureau of Asian Research, May 2013, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf (accessed September 30, 2013), and "The Economic Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies, July 2013, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf (accessed September 30, 2013).

[2] Cyber Intelligence Sharing and Protection Act, H.R. 3523.

abuse these systems and cause a potentially deadly breakdown of the machines or operations that these computers control.

If a supervisory control and data acquisition (SCADA) system, which is used to control various utility and industrial plants, was accessible via the Internet but had no form of login protection, that would be a vulnerability. Of course, more complicated vulnerabilities exist that involve buggy software coding or the ability to bypass authentication procedures.[3] It makes obvious sense for companies and the government to share information about these vulnerabilities so that others who are not yet privy to the information can avoid exposing themselves to unnecessary harm.

The other three clauses refer to efforts to harm or gain unauthorized access to a system or information about a system. These threats can take many different forms, including but not limited to:

- Malware or compromised software,
- Malicious or compromised hardware,
- Attacks that overload the resources or capacity of system such as distributed denial-of-service (DDOS) attacks,
- Insider attacks or espionage,
- Social engineering and phishing,
- Code injection, and
- Targeted and advanced persistent threats.

Often, several of these threats will be used together—for instance, by using an insider to plant malware or malicious hardware on a network to enable an outside hacker to access the compromised network and steal information. Additionally, these threats usually target a weakness or vulnerability. These threats are continuously changing as hackers develop new forms of malware to avoid detection, new schemes to overload a system, and countless other new techniques. Indeed, in 2012, various cybersecurity firms found between 100,000 and 200,000 new versions of malware every day.[4] As a result, information sharing needs to share the latest data on all threats, whether these attacks target webpages, use e-mails to spread malware, or use other methods.

Understanding Cyber Attacks and Threats

Cyber threats can take a variety of forms and it is important to understand how these threats work, so that the critical role of information sharing is recognized. Legislators and civilians who are called upon to understand the problem necessarily need a guide to the conflict domain. At the risk of oversimplification, the following is a short summary of terms to provide context for this discussion:

- **Malware:** Malware stands for "malicious software" and includes viruses, worms, Trojans, bots, rootkits, spyware, ransomware, and many other types of attacks.[5] Malware often has the ability to replicate and spread with little or no help from human users. Malware can either hide in

[3] A high-profile example of such vulnerabilities: In January 2013, the Computer Emergency Readiness Team (CERT), a Department of Homeland Security organization, recommended that users disable Java, a software program that is used by some websites to run interactive games and applications. CERT warned: "This and previous Java vulnerabilities have been widely targeted by attackers, and new Java vulnerabilities are likely to be discovered. To defend against this and future Java vulnerabilities, consider disabling Java in web browsers until adequate updates are available." U.S. Computer Emergency Readiness Team, "Alert (TA13-010A) Oracle Java 7 Security Manager Bypass Vulnerability," January 10, 2013, http://www.us-cert.gov/ncas/alerts/ta13-010a (accessed September 30, 2013).

[4] "Infographic: The State of Malware 2013," McAfee, April 1, 2013, http://www.mcafee.com/us/security-awareness/articles/state-of-malware-2013.aspx (accessed September 30, 2013); AVTest, "Statistics: Malware," 1994 to 2013, http://www.av-test.org/en/statistics/malware/ (accessed September 30, 2013); and "2012 by the Numbers: Kaspersky Lab Now Detects 200,000 New Malicious Programs Every Day," Kaspersky Lab, December 10, 2012, http://www.kaspersky.com/about/news/virus/2012/2012_by_the_numbers_Kaspersky_Lab_now_detects_200000_new_malicious_programs_every_day (accessed September 30, 2013).

[5] These colorful terms all have rather specific meanings. Some, like "ransomware," one can understand from the name itself. Others, like a "rootkit," are more technical and obscure. For a nice guide to the bestiary of malware, see Roger A. Grimes, "Your Quick Guide to Malware Types," *InfoWorld*, December 23, 2012, http://www.infoworld.com/d/security/your-quick-guide-malware-types-205450?page=0,0 (accessed September 30, 2013), and Symantec Corporation, *2013 Internet Security Threat Report*, Vol. 18 (April 2013), http://www.symantec.com/security_response/publications/threatreport.jsp (accessed September 30, 2013).

the background like spyware (software that surreptitiously steals information) or be aggressively obvious like ransomware (software that announces itself and insists on payment of a ransom to have it removed), or it can be a virus that erases entire hard drives.

- **Malicious or compromised hardware:** Hardware threats are less known and can be difficult to identify. Usually purchased from a less than reputable vendor, compromised hardware can contain malicious circuitry that is designed to fail at certain times, in certain places, or on demand. Hardware can also serve as a backdoor for the introduction of malware.[6] This may also be a strategic way for adversary nations to compromise American cyber systems.

- **Overloading system resources:** Billions of computers are attached to the Internet, with access to millions of different websites.[7] When too many computers request to visit a website, the website will slow down or even fail. Denial-of-service (DOS) attacks send a flood of flawed or partial requests to a website to which the website is unable to respond effectively. These requests build up and eventually cause the site to slow down or crash. DOS attacks can be strengthened when a hacker places bot malware on thousands of other computers. These otherwise innocent computers will then do the bidding of the hacker, sending these faulty requests to the website in what is known as a distributed DOS or DDOS attack.[8]

- **Insider attacks:** Many cyber attacks are conducted by employees, contractors, or other people with inside access to an organization, for whom it is easy to steal digital information or create a vulnerability so that a hacker can gain access to the company's system.

- **Social engineering:** Often the weakest links in cybersecurity are regular people, not the firewall or the security system. Social engineering and phishing target individuals by trying to trick an individual into disclosing sensitive information, opening a dangerous attachment, or going to a malicious website by pretending to be someone the individual knows. Spear-phishing attacks are among the most dangerous forms of social engineering, targeting specific groups of people, such as those working at the same company, attending the same university, or using the same bank. By using some piece of inside information about the group, such as referring to a recent company event, the hacker may fool the targets into giving up personal information.

- **Code injection:** Often used to attack a webpage, code injections use a vulnerability in coding to cause a website to do something it was not meant to do. For instance, code could be injected into a public comments section that allows a hacker to push malware onto the computers of anyone merely viewing the message board. Other types of code injection, such as structured query language (SQL) injection, can manipulate coding on a Web form to get that website to allow the hacker access to the contents of a database connected to that site.[9]

- **Targeted and advanced persistent threats:** As the name implies, some bad actors use advanced and specifically tailored versions of the described types of malware in combination with each other to persistently attack a target or group of tar-

[6] John Villasenor, "Ensuring Hardware Cybersecurity," The Brookings Institution, May 2011, http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity (accessed September 30, 2013).

[7] Rod Soderbery, "How Many Things Are Currently Connected to the 'Internet of Things' (IoT)?" *Forbes*, January 7, 2013, http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/ (accessed September 30, 2013), and Julie Bort, "How Many Web Sites Are There?" *Business Insider*, March 8, 2012, http://www.businessinsider.com/how-many-web-sites-are-are-there-2012-3 (accessed September 30, 2013).

[8] U.S. Computer Emergency Readiness Team, "Security Tip (ST04-015): Understanding Denial-of-Service Attacks," February 6, 2013, http://www.us-cert.gov/ncas/tips/ST04-015 (accessed September 30, 2013).

[9] U.S. Computer Emergency Readiness Team, "SQL Injection," 2009, http://www.us-cert.gov/sites/default/files/publications/sql200901.pdf (accessed September 30, 2013).

gets. Such strategies are often the work of nation-states or large criminal-hacker enterprises with significant amounts of resources.[10]

Sharing Advances Security and Privacy

Many of these threats, such as malware and social engineering attacks, strike through e-mails, and it is important that companies share information on these e-mail-based threats to better protect the company, their employees, and their customers. Sharing information about e-mail threats cannot be an open door to all e-mail messages or the personal information they contain; however, e-mails that contain no malware threats must not be shared. Symantec's yearly threat study found that only one of every 291 e-mail messages contained a virus and that one of 414 were phishing attempts, meaning that the vast majority of e-mails pose no cyber threat and will not be involved in any information sharing.[11] E-mail messages with viruses and malware will be analyzed, and the coding of the threat will be shared with others.

For example, an e-mail may have a piece of malware attached as a file or include a disguised link to a malicious website. Cybersecurity personnel will analyze the digital 1s and 0s that make up the malware to see exactly what it does, especially if it is a new type of threat, and then share that information with others so that they can watch out for that threat. Such sharing is not particularly concerned with the content of the message, though in the cases of social engineering e-mails, portions of the text may be needed to inform others of the specifics of that attack.[12] Ultimately, the personal contents of an e-mail, the e-mail addresses, and names of individuals are not typically included in information sharing because they are not necessary for understanding and defeating cyber threats.

While many attacks come through e-mail, the new trend is Web-based attacks, which involve malicious websites or hackers who attack normal sites to steal information from databases connected to the site or to harm site visitors who unknowingly allow malicious software to execute on their own machines.[13] When attacking a website, hackers seek to steal information, harm business operations, or make political statements. Regardless of the kind of attack, personal information may be compromised by attacks on these websites and their connected databases.

Sharing information about cyber threats, vulnerabilities, and IP data enhances and protects the privacy of Internet users.

Similar to dealing with e-mail threats, sharing information about these types of threats need not include personal or sensitive details, but is focused on the vulnerabilities in coding or the source of these malicious attacks. This information can help other companies repair vulnerabilities in their systems or prepare for a potential incoming attack. Network flow data—a record of which Internet Protocol (IP) addresses contacted a network and additional details about the amount and timing of such contacts—can be important to locating an infected computer or finding attackers and their targets. Flow data is also important to law enforcement and government security experts in identifying and stopping hackers, though, pursuant to the Electronic Communications Privacy Act (ECPA), a warrant or court order is needed to link an IP address to a person.[14]

[10] Symantec Corporation, "Advanced Persistent Threats: A Symantec Perspective," 2011, http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf (accessed September 30, 2013).

[11] Symantec Corporation, *2013 Internet Security Threat Report*, Vol. 18, p. 11.

[12] Information Technology Industry Council, "Understanding the Issue: Information Sharing 101," http://www.itic.org/dotAsset/9f0a5a60-ac7e-4fe0-be3e-928806776f28.pdf (accessed September 30, 2013).

[13] Dell SecureWorks Counter Threat Unit, "2012 Threatscape Report," 2013, p. 2, http://www.secureworks.com/assets/pdf-store/other/2012.threatscape.report.pdf (accessed October 1, 2013), and Chris Wysopal, "Web-Based Threats Finally Getting the Respect They Deserve?" Veracode blog, April 23, 2013, http://www.veracode.com/blog/2013/04/web-based-threats-finally-getting-the-respect-they-deserve/ (accessed October 1, 2013).

[14] Information Technology Industry Council, "Understanding the Issue: Information Sharing 101."

When sharing information about any of these threats, cybersecurity experts share technical data about specific cyber attack incidents, such as:

- Tactics, techniques, and procedures used by an adversary;
- The target or vulnerability the enemy is trying to exploit;
- Evidence that shows an attack to be part of a campaign of cyber attacks;
- Indicators that point to a certain hacker or type of hacker; and
- Courses of action to mitigate or fix cyber vulnerabilities.[15]

While these details are important, a standardized way of rapidly transmitting this information is also important. To this end, the Department of Homeland Security (DHS) is sponsoring the nonprofit Mitre Corporation's efforts to develop the Structured Threat Information eXpression (STIX) as the common language and mechanism for quickly analyzing, sharing, and receiving cyber threat information. As STIX or another standard for sharing information becomes more widely used and accepted, the sharing of technical cyber threat details will become easier, faster, and more helpful to cybersecurity efforts. The adoption of a common sharing standard will also improve privacy as the standard will provide clear guidelines for what is to be shared—that is, cyber threat and vulnerability information—and what is not, such as personal and extraneous information.[16]

Information sharing is a relatively inexpensive way of dealing with cybersecurity threats, and it does not involve sharing every piece of, or even most, personal information. While sensitive and personal data on e-mails and in databases may be the target of cyber attacks, information sharing is not aimed at using the personal content of those e-mails and databases because that information does nothing to support security. Instead, sharing information about threats, vulnerabilities, and IP data enhances and protects the privacy of Internet users.

It is worth emphasizing that information sharing is not a panacea. It will not enable private-sector actors or the government to avoid all threats. Some vulnerabilities are unknown and others are poorly understood. But information sharing is a simple and effective way of improving cybersecurity. It is the "low-hanging fruit" of greater protection—yet we cannot seem to grasp it.

Enabling Real Information Sharing

Given that cybersecurity threats are very real and costly and that voluntary information sharing is an inexpensive and privacy-enhancing way of staving off these threats, Congress should consider ways to facilitate sharing. There are three ways that Congress can enable information sharing:

1. **Remove barriers and ambiguities** in existing law to clearly allow the sharing of cybersecurity information,
2. **Provide those who share information** with robust liability protection from criminal and civil penalties, and
3. **Require that shared information** be unavailable under FOIA or for use by regulators.

Removing Barriers and Ambiguities. Currently, some private organizations would be interested in sharing information with others in the private sector and the government to promote cybersecurity but do not do so because of ambiguities in out-

[15] Sean Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)," The MITRE Corporation, 2013, http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf (accessed October 9, 2013).

[16] It is also worth emphasizing the speed at which information sharing needs to take place. Cyber threats flow through the Internet at near-instant speeds, so defenses must be this fast as well. Human analysis and action is often the slowest part of the process. The STIX standard can allow information to be shared rapidly with other organizations in a way that allows those organizations' machines to read that new information and act on it as soon as it is received, cutting out much of the slower human analysis. Security that responds at machine speed, rather than human speed, while not fully realized yet, is an important step that STIX can help to advance. Of course, STIX or a similar system has not been universally adopted or incorporated into commercial off-the-shelf technology, and until then, sharing will not be as powerful as it could be. For more, see Kelly Jackson Higgins, "Attack Intelligence-Sharing Goes 'Wire-Speed,'" Dark Reading, December 5, 2012, http://www.darkreading.com/vulnerability/attack-intelligence-sharing-goes-wire-sp/240143864 (accessed October 9, 2013).

dated communications laws. Specifically, the Wiretap Act and the Stored Communication Act seem to prohibit or potentially prohibit the sharing of cybersecurity information.[17] These two titles, though created with the important purpose of protecting the privacy of citizens' communications, were initially passed in 1986 to deal mostly with telephone issues. These sections of ECPA prohibit electronic communications providers from disclosing the contents of electronic communications or information about a customer without having the appropriate authorization.[18] Of course, this could be and is being construed by many to include the coding of viruses and malware and the IP addresses from which cyber attacks are originating. While there are exemptions in these laws that might be read to authorize information sharing, ultimately businesses will be hesitant to do something that could be illegal.

With such outdated laws applying to Internet communications, companies in possession of cyber threat and vulnerability information are hesitant to share information due to fear of legal repercussions. Until these laws are updated or other protections are provided through legislation, these ambiguities will continue to inhibit information sharing.

Providing Appropriate Liability Protection. In addition to ambiguities of current law, other legal concerns also restrict the sharing of cybersecurity information. If a company shares information without malicious intent but the information is mistaken, the company fears it will be sued for damages resulting from the error. Additionally, if a company shares information about a potential breach out of an abundance of caution and a desire to help others, it could end up facing civil or criminal charges. The Information Technology Industry Council (ITI) provides a useful summary of why liability concerns hamper information sharing. ITI writes that "Company A [could] voluntarily report what may be a cybersecurity incident in an information-sharing environment, such as in an ISAC (Information Sharing and Analysis Centers), or directly to the government, such as to the FBI." Based on such sharing,

> government prosecutors, law enforcement agencies, or civil attorneys [could] use this information as the basis for establishing a violation of civil or criminal law against Company A or a customer, partner, or unaffiliated entity harmed by the incident sues Company A for not informing them of the incident as soon as they were aware of it. Company A's disclosure can be seen as a "smoking gun" or "paper trail" of when Company A knew about a risk event though Company A did not yet have a legal duty to report the incident. Such allegation could lead to costly litigation or settlement regardless of its validity.[19]

In these and many other situations, an organization can merely share information and end up getting hit with a lawsuit.[20] The current lack of protection is one of the biggest obstacles to information sharing, as evidenced by many companies' and trade organizations' statements.[21]

To remove this obstacle, information sharers should receive strong liability protections. More specifically, protection needs to apply as long as the sharers of information were not acting with malicious intent or gross negligence. Such a standard sounds similar to a standard of "good faith," but it is actually

[17] For more on these barriers, as well as more information about cyber information sharing generally, see Ryan Radia, "Reforming Legal Hurdles to Cyber Threat Information Sharing," George Washington University Law School, 2013. Available from authors upon request.

[18] Paul Rosenzweig, "Cybersecurity and Public Goods: The Public/Private 'Partnership,'" in Peter Berkowitz, ed., *Emerging Threats in National Security and Law* (Stanford, CA: Hoover Institution, 2011), http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf (accessed October 1, 2013).

[19] Information Technology Industry Council, "ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing," January 2012, http://www.itic.org/dotAsset/fae2feab-7b0e-45f4-9e74-64e4c9ece132.pdf (accessed August 7, 2013).

[20] Sharing information about a violation of law does not excuse the violation but merely prevents the information from being used against the sharing organization. While evidence pointing to a violation may be shared by an organization, that does not preclude an investigation from finding that or other evidence through different means.

[21] U.S. Chamber of Commerce, "Critical Infrastructure Protection, Information Sharing and Cyber Security," November 4, 2013, https://www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security (accessed February 14, 2014); Information Technology Industry Council, "ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing;" and Casey Wooten, "NIST Official: Businesses May Need Tax Breaks, Immunity to Adopt Cyberstandards," Bloomberg BNA, May 27, 2013, http://www.bna.com/nist-official-businesses-n17179874217/ (accessed October 1, 2013).

stronger and prevents wasteful and frivolous lawsuits. "Good faith" sounds like a reasonable standard, but nearly any trial lawyer could find a way to accuse an organization of bad faith and take it to court for sharing information. A requirement of presenting evidence of malicious intent is a more appropriate standard to encourage information sharing.

Protecting Information from FOIA and Regulatory Use. Another hindrance to effective cybersecurity information sharing is the fear that government regulators or competitors will use shared information to hurt the sharer's business. Similar to liability protection, protection from regulatory use guarantees that a regulator will not use shared information to propose additional regulations or punish a potential failure to meet regulatory standards of which the government would have been otherwise unaware. An example of why regulatory protection is needed: If a company shared information about a potential breach of its systems only later to find that "a database was compromised that included Individually Identifiable Health Information as defined under the Health Insurance Portability and Accountability Act (HIPAA)," the Federal Trade Commission could then use the shared information "as evidence in a case against [that company] for violating the security provisions of HIPAA."[22] Under regulatory-use protection, businesses will not be afraid to share information on breaches and cyber attacks.

FOIA protection is also necessary because businesses do not want their competitors to get their hands on proprietary information or business dealings. In the event of a breach, businesses may share information about a trade secret that may have been compromised in the hope that the government can help discover who stole that secret and prosecute the theft. Without protection, a competitor could submit a FOIA request for that information and possibly find out something about the trade secret or the company's business dealings. At the very least, the competitor could announce that the original company had been breached, forcing that company to deal with bad press and lost customers.[23]

Finally, any information shared should not be used for anticompetitive behaviors. Firms that engage in anticompetitive activities should be subject to civil penalties, though the liability standard should be set high here as well. On the other hand, the legislation should make clear that the sharing of cybersecurity threat and vulnerability information is not in itself anticompetitive. While some telecommunications companies have expressed the fear of antitrust liability for information sharing, the law should make clear that such sharing is not subject to liability because it is not intended for economic advantage. That caveat should likewise enable liability when sharing entities go beyond the purposes for which the sharing is done to seek economic advantage.

Clearing up legal ambiguities and providing businesses with strong liability, FOIA, and regulatory-use protections will allow organizations to share information with little fear of damaging repercussions. This allows the private sector and government to contribute actively to and learn from others and collaboratively defend U.S. computers and networks.

Creating a Framework for Effective Sharing

While removing barriers to information sharing is important, more must be done to facilitate timely and multi-directional sharing of information. In other words, there needs to be a clear framework for how organizations, both in and out of government, can voluntarily share cyber threat and vulnerability information. There are many forms that such a framework could take.

One option is a "Post-to-all." Post-to-all models are essentially listservs that allow entities in the group to quickly post information to other members of the group. The advantages of such an approach

[22] Information Technology Industry Council, "ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing." On the topic of health records being hacked, it is worth noting that implementation of the Affordable Care Act's online data hub has experienced serious technical difficulties and was not subjected to rigorous security tests. Since this system will serve as the conduit for millions of individuals' personal information, the fact that security tests and measures are not yet in place is a major concern. For more information, see David Inserra, "Cyber Failures in Obamacare Exchanges: Dangerous to Your Wallet and Privacy," The Heritage Foundation, *The Foundry,* October 2, 2013, http://blog.heritage.org/2013/10/02/cyber-failures-in-obamacare-exchanges-dangerous-to-your-wallet-and-privacy/.

[23] Information Technology Industry Council, "ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing," and Paul Rosenzweig, "Cybersecurity Information Sharing and the Freedom of Information Act," testimony before the Committee on the Judiciary, U.S. Senate, March 13, 2012, http://www.judiciary.senate.gov/pdf/12-3-13RosenzweigTestimony.pdf (accessed October 1, 2013).

are that sharing happens very quickly and at virtually no cost. However, it is up to each organization to analyze information and decide what is useful. Additionally, if such an approach is used on a large scale, some sharers may not trust everyone in the group, thus weakening buy-in to sharing.[24] On a small scale, however, trust and a common understanding of what kind of information is most valuable can be established more easily, thus enhancing the cybersecurity of those organizations.

Under regulatory-use protection, businesses will not be afraid to share information on breaches and cyber attacks.

An alternative model of sharing might be called "hub-and-spoke." Hub-and-spoke models allow organizations to send information to a common hub, which then organizes and possibly analyzes the information before passing it to other organizations. Currently, the United States has public-private Information Sharing and Analysis Centers (ISACs) that generally operate within each sector of industry. Additionally, some federal organizations like the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) act as distributors of cyber information, though there is not a clear federal hub yet. There are weaknesses in such a model, however. A hub can slow sharing and can cost more than post-to-all models, though it is still relatively inexpensive. Additionally, the credibility and effectiveness of the hub is of the upmost importance.[25] If it does not function well, other organizations will not fully invest and participate in information sharing. Such is evident in the case of DHS, where a lack of skilled personnel and leadership has prevented the department from fully taking the national lead on cybersecurity.[26]

Both models have their place, and both should be encouraged. A post-to-all model might be most appropriate for a group of companies that have established trust among themselves and are dealing with similar issues. This arrangement can and should develop organically as different organizations feel necessary. In addition to existing ISACs and direct cooperation between companies and government agencies, a more formal hub-and-spoke arrangement should be established to allow as many organizations as possible to participate in the exchange of cybersecurity information. This hub should aggregate information not just from the private sector, but also from the government. Neither the government nor the private sector has all the answers and sees all the threats, so it is critical that this hub receive information from both. Since it will be receiving and sending information to a wide variety of sources, the hub can also adopt STIX or a similar system and push a standardized information-sharing and analysis language into widespread use within the government and private sector. Additionally, while some government information is rightly classified and should be shared only with cleared individuals, it is important that equal time is spent on transmitting non-classified data to and from the hub as well.

Where this organization should be housed is a topic of great discussion. In the last Congress, Senator John McCain's (R–AZ) proposed SECURE IT bill made the NSA the hub of information sharing because it has the most expertise and resources. Several other bills, including the proposed Cyber Intelligence Sharing and Protection Act (CISPA), make the NCCIC the hub because a civilian agency is the most appropriate place for oversight of civilian networks. To avoid turf wars and the exclusion of valuable analysts and resources, the more appropriate location for a national-level hub would be a nonprofit, public-private partnership. Such an organization would be managed by representatives from the NSA, DHS, privacy groups, industry, and other stakeholders. This approach to management would allow agencies and stakeholders to cooperatively oversee the sharing that occurs through the hub, making sharing more transparent and the shared information more trustworthy.

[24] The MITRE Corporation, "Cyber Information-Sharing Models: An Overview," October 2012, http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf (accessed October 1, 2013).

[25] Ibid.

[26] David Perera, "DHS Cyber Has Problems with Hiring, Not Retention, Says Stempfley," FierceGovernment IT, May 18, 2013, http://www.fiercegovernmentit.com/story/dhs-cyber-has-hiring-not-retention-problem-says-stempfley/2013-05-18 (accessed October 1, 2013).

As mentioned, such an organization would cost a relatively modest amount.[27] With U.S. government spending a constant concern, it would be unwise for the government to cover the entire cost of the program. On the other hand, pushing the entire cost to the private sector would discourage its use. Since both private-sector and public-sector cybersecurity efforts benefit from information sharing, government stakeholders such as the NSA and DHS should be required to pay at least half of the cost of operating the hub. The remaining portion should be charged to the private-sector stakeholders with a fee that corresponds to the size of the company and the level of information usage. Such an arrangement ensures that smaller companies are not discouraged by a large fee, while larger companies and cybersecurity providers, who have more to protect, pay a larger amount. Regardless, this fee will be relatively minimal. To encourage organizations to participate in the program, the federal government may need to pay these costs initially and then eventually share the costs of this public-private partnership with the private sector.

To be sure, there are challenges with this third-party hub mode. Some are concerned that information sharing on a national scale will almost certainly involve speed, volume (in number and size of transactions), and complexity requirements beyond what such a hub is capable of today. The third-party hub model may also run afoul of a sunk-costs problem: Private-sector actors who would be affected—such as ISACs, the NCCIC, and the National Cyber Investigative Joint Task Force (NCIJTF)—have invested a great deal of time and effort in the current sharing framework and are not interested in devoting any resources to creating a new framework.

Reluctance to break with the current model is certainly understandable, but the justification for legislation, if it exists at all, is that the current model is not effective. There seems to be little virtue in continuing to adhere to the current ad hoc approach simply because of inertia and resistance to change.

More to the point, wholesale change is the least bad alternative, notwithstanding the cost. The only other option for a hub-system is to centralize sharing in DHS since, as noted, authorizing the NSA to serve as a federal hub is an impractical solution. Such a solution would require a significant investment of resources at DHS to enable the department to take the lead and become a fully capable actor in this domain, eliminating the current bottlenecks and bureaucratic inertia. Even then, it is questionable whether or not DHS is up to the task. Given this reality, it seems as though the most likely way to accomplish the information-sharing objective would be through unwieldy mandates that *require* the private sector to share information with DHS fully and continually. While the third-party model is politically impractical, it seems no less impractical than planning for significant improvements in DHS capabilities.

Using Information Sharing to Stop Threats

Once the barriers and ambiguities have been removed and a framework established, the real business of cybersecurity information sharing can begin. Most private-sector companies will receive an injection of actionable information on cybersecurity.[28] Of greater concern is how the government uses the shared information: While the overwhelming majority of uses will be focused on cybersecurity, should that information be available for other uses?

The federal government should be authorized to share information as long as a significant purpose for sharing the information is a cybersecurity purpose. The purpose of such broad sharing is to ensure that an agency of government is not excluded from receiving information that might in some way help to prevent harm.

[27] U.S. CERT, which makes up most of the NCCIC, was budgeted $79.1 million in 2013. CERT not only shares cyber information with U.S. organizations, but also analyzes threats, responds to cybersecurity incidents, and provides technical assistance to information-system operators. Given all the extra responsibilities that CERT has, it is reasonable to estimate that the recommended organization, which would be focused purely on aggregating, sorting, and distributing cybersecurity threat and vulnerability information in the U.S., will cost substantially less. Furthermore, since in 2008, there were over 11,000 firms with more than 1,000 employees and over 125,000 firms with at least 100 employees, according to the U.S. Census Bureau, the private sector's share of such a clearinghouse will be split many ways. As a result, the cost per company will likely be minimal. See U.S. CERT, "About Us," http://www.us-cert.gov/about-us (accessed November 25, 2013), and U.S. Census Bureau, "Statistics About Business Size," http://www.census.gov/econ/smallbus.html (accessed October 21, 2013).

[28] As mentioned earlier, these companies should be prohibited from using shared information to harm their competitors or to engage in any other anti-competitive behavior.

There could be, for instance, a malicious code discovered in U.S. and allied military systems in a specific region that would shut down those systems on a specified time and date. It would be foolish not to connect the cybersecurity and national security dots to figure whether a major "real life" attack might be planned in conjunction with the cyber attack. Closer to home, a bank could find out that its computer system for controlling physical security at one of its branches had been penetrated. Once again, this would be a cybersecurity problem that is probably not strictly a cyber threat. Cyber and non-cyber law enforcement agencies should be brought in to investigate the very real possibility that bank robbers may be targeting that branch for a heist. Of course, most cyber issues will remain just cyber issues, but to prevent the government from using that information to stop other, physical crimes and attacks is simply unwise. Such a restriction on using information would be a return to the pre-9/11 mindset, where information was bottled up in each agency and not shared—largely for nonsensical bureaucratic reasons. Information should be available for broad uses. The information shared is, in essence: lines of code, the origins of these attacks, and the targets of these attacks. Broad sharing helps defend the liberty of Americans not just in cyberspace, but also in the real world.

Clear and Responsible Oversight

All that said, it is important that any information-sharing proposal ensure strong oversight of the information-sharing system that is established. As with any government program, the potential for abuse is real. Personal information could be inappropriately shared or used. For this reason, the United States has placed privacy officers throughout government agencies since 9/11 to review various new security and information-sharing programs.[29] The U.S. should use this existing system of privacy officers to review sharing procedures and observe how information is being used. The information-sharing hub will have privacy groups on the board not only to review official sharing procedures, but also to analyze information sharing that occurs and its effects on privacy. Additionally, a yearly report on any privacy violations and the functioning of the system should be filed by the U.S. Government Accountability Office (GAO) and presented to Congress.

> There seems to be little virtue in continuing to adhere to the current ad hoc approach to cybersecurity simply because of inertia and resistance to change.

While it is important that oversight be strong, it is also important that it not be duplicative or restrict the legitimate sharing and use of proper information. For example, any requirement for complete anonymization of all information that is shared, though ideal, would cause delays in the sharing process, thus rendering any information less useful. Anonymization that can be done quickly and not hinder the sharing of information, however, should be encouraged. It is worth repeating that most shared information will contain no personal information at all since cybersecurity measures are aimed at technical threat indicators, the digital 1s and 0s of malware, Web attacks, and other threats.

Real Cybersecurity Requires Strong Information Sharing. Cyber threat and vulnerability information is a valuable resource in combating malicious cyber actions, and this resource should be shared with and used by others. To better enable cyber information sharing, Congress and the Administration should:

- **Clearly define information sharing and its benefits.** Recent revelations and allegations about various counterterrorism programs have Americans rightfully concerned about their privacy and civil liberties. These concerns can and should be addressed by officials in government, explaining why these programs do not infringe on an individual's liberty and serve a crucial role in defending the United States—and that same individual—from terrorism. The same is true of cybersecurity information sharing. A thoughtful examination of the facts answers most concerns,

[29] Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110–53, and 6 U.S. Code § 142 and 345.

and these facts should be clearly and regularly articulated by the government. To this end, any information-sharing bill should contain a clear explanation of what kind of information can be shared and how it can and cannot be used.

- **Remove ambiguities and restrictions in current law against sharing cybersecurity information.** Provisions of law passed in 1986 seem to prohibit the sharing of cybersecurity information. These provisions should be revised to account for the modern-day need for cyber information sharing. Alternatively, Congress could include an exception to those provisions in any cybersecurity bill through language such as: "Notwithstanding any other provision of law, U.S. organizations are authorized to share cybersecurity threat and vulnerability information."

- **Protect those who share information with strong liability, regulatory, and FOIA safeguards.** Companies that want to share information need to be protected—otherwise, they will not readily share such information. Congress should provide robust protection from liability, placing the burden of proof on the accuser to demonstrate that the information was shared with malicious intent or gross negligence. Congress should also prohibit regulatory agencies from using shared information against the regulated company or community. Similarly, Congress should prohibit FOIA requests for shared information so that third-party companies do not use information sharing as a way to harm or steal from their competitors.

- **Create a framework for information sharing that facilitates rapid, multidirectional sharing.** The mere act of allowing information sharing will not ensure that other organizations across the country receive the information in a timely manner. Congress should establish a national hub for information sharing to act as a clearinghouse of information using a standardized language such as STIX to streamline cybersecurity analysis and enable action at machine speed. This hub should be a private-public partnership that includes stakeholders from relevant government agencies, privacy groups, and industry. The small cost of running this cooperative organization should be funded by splitting the cost between the government and private groups. Additionally, Congress should encourage the continued role of industry-focused ISACs as well as sharing directly between two or more organizations or agencies.

- **Allow information to be shared and used broadly.** Once the government has cyber information, it is important that it be allowed to use that information for other purposes, such as a criminal investigation, so long as a significant purpose of sharing the information is for advancing cybersecurity. While broad authorization may raise privacy concerns, the information in question does not generally include any content or sensitive personal details. As a result, the broad authorization will not be a threat to the privacy or liberties of Americans, but will defend and enhance Americans' security and liberty.

- **Provide robust but not restrictive forms of oversight.** Information sharing should be designed in a way that does not infringe on the liberties of Americans—and strong oversight of the information-sharing process should also be established to ensure that civil liberties remain protected. Existing privacy officers and boards within U.S. government agencies should be tasked with reviewing information-sharing procedures and examining particular cases in which information is shared. Together with annual reports by an independent organization (perhaps, the GAO), the U.S. can ensure that cyber information sharing is being done correctly—efficiently and responsibly. Any additional layers of oversight or obstructive requirements, however, will merely slow information sharing and make the United States less secure.

Advancing U.S. Cybersecurity, Liberty, and Prosperity

Cybersecurity threats against the United States are real and costly. The U.S. must do more to counter cyber threats, but any policies must first do no harm and promote real security. Information sharing accomplishes these goals by providing government and private-sector organizations with data and intelligence on the latest cyber threats and vulnerabilities that can then be used to mitigate or prevent those dangers. With proper protections, frameworks, and oversight, the United States can take advantage of this cost-effective and dynamic form of security.

*—**David Inserra** is a Research Associate for Homeland Security and Cybersecurity and **Paul Rosenzweig** is a Visiting Fellow in the Douglas and Sarah Allison Center for Foreign and National Security Policy, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*