



Cyber Threat Information Sharing

Recommendations for Congress and the Administration

AUTHORS Denise E. Zheng | James A. Lewis



Cyber Threat Information Sharing

Recommendations for Congress and the Administration

Authors

Denise E. Zheng
James A. Lewis

A Report of the CSIS Strategic Technologies Program

March 2015

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Former U.S. senator Sam Nunn has chaired the CSIS Board of Trustees since 1999. Former deputy secretary of defense John J. Hamre became the Center's president and chief executive officer in 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible by the generous support of the American Bankers Association, the Depository Trust & Clearing Corporation, the Financial Services Information Sharing and Analysis Center, and Soltra Solutions, LLC.

© 2015 by the Center for Strategic and International Studies. All rights reserved.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Cyber Threat Information Sharing

Recommendations for Congress and the Administration

Denise E. Zheng and James A. Lewis

As technology and the Internet continue to evolve and grow in complexity, so, too, does the nature of cyber attacks. The economics of cyber attacks are skewed to favor the attacker: exploits are easily acquired and can be reused on multiple targets, and the likelihood of detection and punishment is low. Adversaries range from lone hackers to well-resourced criminal enterprises and nation-state groups who seek to steal personal data and intellectual property, and perhaps, to disrupt or sabotage critical infrastructure. Companies and governments are engaged in an increasingly difficult battle against persistent and agile cyber adversaries. Under these conditions, reactive strategies are insufficient to deal with the threat. Improved information sharing is critical to effective cyber incident detection and response by reducing duplication of effort and enabling one organization's detection to become another organization's prevention.

Cyber threat information sharing is not a cure-all solution, but it is a critical step toward improving cyber defenses. The benefits of information sharing, when done correctly, are numerous. Sharing enables organizations to enhance their cyber defenses by leveraging the capabilities, knowledge, and experience of a broader community. It can provide better situational awareness of the threat landscape, including a deeper understanding of threat actors and their tactics, techniques, and procedures (TTPs), and greater agility to defend against evolving threats. It can improve coordination for a collective response to new threats and reduce the likelihood of cascading effects across an entire system, industry, sector, or across sectors.

In recent years, several federal efforts have promoted the sharing of cyber threat information between the private sector and government. Examples include the Department of Homeland Security's (DHS) Cyber Information Sharing and Collaboration Program (CISCP) and the Federal Bureau of Investigation's (FBI) Infraguard, which share cyber threat information with a broad community of industry stakeholders. The Defense Industrial Base Cyber Pilot, which merged with DHS's Enhanced Cybersecurity Services (ECS) program in 2013, and the Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) are more targeted

programs that share sensitive or classified cyber threat information with certain industry partners.

Information-sharing partnerships have also grown organically out of the private sector. Information Sharing and Analysis Centers (ISACs) serve as important venues for cyber threat information sharing between private companies, with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) being the most operationally mature. The success of these programs is due, in large part, to existing relationships of trust within these sectors, shared business models, and common goals.

Not all cyber threat information-sharing partnerships have been effective. Programmatic, technical, and legal challenges, as well as lack of buy-in from the stakeholder community, are the key impediments. President Obama's Executive Order, "Promoting Private Sector Cybersecurity Information Sharing," attempts to address these challenges by encouraging the development of "information sharing and analysis organizations" (ISAOs), establishing voluntary standards for these sharing organizations, and streamlining the process for sharing and receiving information from government agencies. The Executive Order is a significant step forward, but its success is dependent on the passage and effective implementation of legislation to address outstanding legal limitations on sharing and companies' concern that sharing cyber threat information could expose them to civil and criminal liability for disclosing sensitive personal or business information.

In recent years, several bills have been introduced in Congress aimed at improving cyber threat information sharing by offering liability protection and access to government-furnished cyber threat intelligence as incentives. None of these efforts has advanced because of concerns about privacy and law-enforcement uses of the information, and disagreement over liability protection and the role of government in information-sharing mechanisms, which fractured support for legislation. The current 114th Congress has a new opportunity to pass legislation and should do so without delay.

Recommendations for Policy and Legislation

In December 2014, the Center for Strategic and International Studies (CSIS) launched a project to identify lessons learned from existing and previous cyber threat information-sharing efforts and outline recommendations for future policy and legislation.

CSIS convened three workshops to discuss the technical, structural, and legal challenges to cyber threat information sharing. A cross-sector stakeholder group with participants from government, industry, and privacy organizations attended the workshops. The workshops included experts from the financial services,

telecommunications, electricity, oil and gas, retail, and commercial information technology sectors, as well as privacy community. Government participants included the Departments of Defense, Homeland Security, Treasury, and Justice, and staff from the National Security Council and Congress.

Based on the comments and suggestions shared at the workshops, CSIS produced a set of recommendations for policy and lawmakers to consider as they develop and implement new cyber threat information-sharing policies and legislation. The recommendations cover both structural and legal issues.

Recommendation 1: Sectors and industries have different risk profiles for cybersecurity. Stronger information-sharing arrangements with the government are appropriate for some private entities but not others.

There is no one-size-fits-all approach to cyber threat information sharing. A single, overarching approach to sharing between the private sector and government will not work. Each sector has unique needs for government involvement, and operates in a different regulatory environment. Information-sharing arrangements between government and private entities should be informed by a cost-benefit analysis that takes into account industry and sector risk profiles.

In understanding industry or sector risk profiles, some possible variables to consider include:

- *Nation-State Involvement:* Organizations that are the target of state-sponsored cyber attacks have a need for closer sharing and collaboration with the government, including access to classified cyber threat intelligence and technical assistance. Some U.S. companies face unique threats because they are the target of well-resourced cyber adversaries backed by criminal enterprises or nation-states. A more government-centric cyber threat information-sharing and incident-response model may be necessary for these industries or sectors.
- *Criticality:* Owners and operators of critical infrastructure, particularly those that provide backbone service or infrastructure, and providers of mission-critical national security capabilities may need stronger sharing relationships with the government. Government has an inherent responsibility to provide national security and economic stability, and to ensure public health and safety. For the most critical systems, robust mechanisms for cyber threat information sharing and collaboration between the government and industry may be necessary.
- *Risk to Privacy:* Some companies, due to the nature of their business, store and process more personal information and communications than others. Sharing information with the government is inherently more complicated for these

companies. A limited or minimized role for government in cyber threat information-sharing arrangements is more appropriate for these entities.

A complete risk profile will include many more elements, but the variables outlined above are a helpful starting point. Entities that face nation-state opponents, are highly critical, and pose a low risk of disclosure of personal information would benefit from greater sharing with the government. Others should focus near-term efforts on sharing between private-sector partners (“private-to-private” sharing) and consider limiting the role for government.

Recommendation 2: Private-to-private sharing with a minimal role for government can help promote voluntary information sharing and alleviate privacy concerns.

Many of the privacy and liability concerns related to sharing cyber threat information can be addressed by minimizing the role of government and encouraging private-to-private information-sharing relationships. This would help address concerns that information could be used by government agencies for regulatory actions or as a backdoor for law-enforcement or intelligence collection activities.

For most organizations, particularly those that store or process large amounts of personal information and communications, day-to-day sharing of cyber threat information should focus on private-to-private sharing without government involvement.

Recommendation 3: Entities should make reasonable efforts to eliminate personal information that is irrelevant to the threat prior to sharing.

There is some personally identifiable information (PII), such as the Internet Protocol (IP) address of an attacker, which is relevant and essential to describing and mitigating the cyber threat. However, PII that is irrelevant to the threat should be removed prior to sharing with other entities. There are legitimate privacy concerns that sharing could lead to unnecessary disclosure of personal information. Many companies already take precautions to remove PII, but there remains concern that sharing could expose companies to potential liability or the threat of suit.

Legislation should require companies to make reasonable efforts to eliminate PII that is irrelevant to the threat prior to sharing and provide liability protections to companies that take such measures.

The National Institute of Standards and Technology (NIST) and DHS should consider identifying best practices for removing PII and issuing guidance on what specific elements of information, some of which may be PII, are relevant to the threat.

Recommendation 4: Build upon existing information-sharing organizations and mechanisms.

Several industry sectors already have Information Sharing and Analysis Centers (ISACs) and decentralized or peer-to-peer sharing relationships that have proven effective. ISACs offer sector-specific perspectives on threats and incidents in addition to providing anonymization.

Rather than creating duplicate entities for sharing, government should support operationalizing and maturing existing information-sharing organizations. For critical infrastructure sectors where ISACs do not exist, government should encourage private-sector efforts to form information sharing and analysis organizations.

Recommendation 5: Streamline procedures for companies to share cyber threat information with the government as well as within and among sectors.

Currently, the sharing of cyber threat information between companies and the government is conducted through Cooperative Research and Development Agreements (CRADAs). Created by the Federal Technology Transfer Act of 1986, the CRADA mechanism was designed to facilitate collaboration between government and private companies for research and development; it was never intended to be used in the context of cyber threat information sharing. CRADAs were an interim measure adopted several years ago to be used until DHS could develop a standard agreement tailored for information sharing.

The CRADA process is lengthy and resource-intensive, requiring significant involvement of companies' legal counsel. The effect is that resource-constrained medium-size and small companies are excluded from sharing arrangements with the government.

Legislation should establish a standardized and streamlined process for companies to enter into collaborative information-sharing arrangements with the government.

Recommendation 6: Cyber threat information shared voluntarily with the government should be protected from disclosure through Freedom of Information Act (FOIA) requests and barred from use in civil litigation or regulatory purposes.

Risk of public disclosure of information shared with the government and potential use of the information in regulatory actions have a chilling effect on voluntary cyber threat information sharing.

The Protected Critical Infrastructure Information (PCII) program run by DHS is a mechanism for ensuring information is protected, but there is a lack of clarity on the types of information covered by the designation and uncertainty in the process. In

some cases, sector-specific regulators request the same information directly from companies after the information was submitted under PCII. Companies may feel obligated to satisfy the request, but the protections provided under PCII do not extend to such sharing, thereby allowing regulators to use the information for regulatory actions.

Legislation should provide clear protection of voluntarily shared cyber threat information from disclosure through FOIA requests and from use in regulatory actions.

Recommendation 7: Identify ways for information sharing models to demonstrate value for all parties involved.

Effective cyber threat information must be actionable. It should be timely, accurate, relevant to the recipient, and specific enough for the recipient to take action in response to the threat.

The one-way flow of information has been one of the most frequent complaints about some current information-sharing arrangements. Although information sharing between entities does not have to be symmetrical, it should be bidirectional and demonstrate value for all parties. Companies cannot be properly incentivized to share cyber threat information unless they receive useful data in return.

Recommendation 8: Centralized and decentralized models for information sharing each have unique benefits. Government should encourage both models for sharing.

Centralized “hub-and-spoke” models for cyber threat information are effective if the hub performs services that increase the value of the information shared. This could mean enriching the data with additional sources or context, validating data for accuracy, or sanitizing data by de-identifying or anonymizing sensitive elements.

Decentralized “peer-to-peer” sharing arrangements between organizations tend to involve a greater degree of trust that parties share common goals and have agreed to a set of rules for sharing. Peer-to-peer sharing arrangements may be more appropriate for targeted, sensitive, or classified information.

Government should encourage both types of sharing and avoid prescribing one over the other.

Recommendation 9: Information-sharing arrangements should take into account the type of information being shared. Sharing technical threat indicators poses little risk to privacy, disclosure of sensitive business information, or regulatory exposure. Sharing more sensitive contextual threat information poses a greater risk to individual privacy and to companies.

There are two basic categories of cyber threat information:

- *Technical threat indicators* (e.g., IP addresses, specific strings of data, and file hashes, exploit toolkits or payloads, and adversary tactics, techniques, and procedures)
- *Contextual threat intelligence* (e.g., exploit targets, exfiltrated content, incident details, and specific courses of action)

Technical threat indicators are specific, common, and repeatable forms of information that readily lend themselves to anonymization, standardization, and rapid forms of distribution. These indicators can be effectively anonymized to obscure the target of an attack. Sharing this kind of information poses low risk of disclosure of personal information or sensitive company and customer information. Technical threat indicators account for the vast majority of threat information that is available. Significant gains can be achieved through automated sharing of technical indicators.

Contextual information—including target information, adversary course of action, and detailed information about the campaign and threat actor—poses a greater risk to privacy, contractual liability, and unauthorized disclosure of classified information. Unlike technical threat indicators, sharing contextual information is difficult to automate and requires more human involvement. One of the benefits of contextual information is that it can help guide investment decisions and strategies by more clearly identifying the threats a company is facing; however, technical threat indicators are arguably more valuable for real-time mitigation activities against immediate threats.

Improved sharing of contextual threat information will require new policies. In the near term, progress can be made by increasing the volume and speed at which technical indicators are shared, and by sharing them across sectors. Improvements in the volume and speed at which cyber threat information is shared and in mitigation response time require automation. It also means that sharing of technical threat indicators should, to the maximum extent possible, conform to open standards for data formats and transport protocols.

Recommendation 10: Permissible law enforcement uses of cyber threat information shared by companies with the government should be restricted to cybersecurity purposes and a limited set of other activities.

The goal of improved cyber threat information sharing is to strengthen cyber defenses and to improve the resiliency of the private sector and the government to cyber attack. In a post-Snowden environment, there is heightened scrutiny and concern over government access to data and how it is used.

Cyber threat information voluntarily shared by private entities with government should be limited to use for cybersecurity purposes and to a limited set of other circumstances, such as to prevent or mitigate imminent threat of death or bodily harm.

Recommendation 11: Legislation should authorize monitoring and sharing of cyber threat information, and provide a safe harbor from civil and criminal liability for good-faith actions in conducting such activities.

The Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA) prohibit communications providers from voluntary disclosure of communications content with the exception of emergency situations or to protect their own networks. Sharing is not directly authorized by law, but is permitted as an exception to a prohibition, which has created uncertainty around the legality of sharing cyber threat information.

In May 2014, the Department of Justice (DOJ) released guidance outlining its interpretation of lawful cyber threat information sharing under existing electronic communications statutes. While DOJ's guidance helped clarify the issue, companies remain concerned about exposure to liability for monitoring and sharing cyber threat information.

Legislation should provide explicit authorization to share cyber threat information and a safe harbor from liability for sharing in good faith. It should also seek to reduce legal uncertainty around lawful countermeasures.

Conclusion

Information sharing empowers organizations to take individual as well as collective action to reduce risks, deter attackers, and enhance overall resilience. Initially, cyber threat information sharing was conducted in an informal, ad hoc manner. Today, sharing of cyber threat information between private companies and with government is more structured, frequent, and regular. However, there are still several outstanding legal and structural challenges to improved sharing, such as concerns about privacy, risk of liability, and the appropriate role of government.

Security and privacy are not mutually exclusive. The security benefits of improved information sharing can be achieved in a manner that still protects privacy and civil liberties. It can also be achieved in a manner that protects PII and company sensitive information as well as other equities.

Improved cyber threat information sharing has many benefits, but information sharing only provides a means for achieving specific goals and outcomes; it is not an end in itself. As such, government and companies should articulate the objectives and

goals for information sharing, and tailor mechanisms for information sharing to achieve those goals.

About the Authors

Denise E. Zheng is a senior fellow and deputy director of the Strategic Technologies Program at CSIS, where her work is focused on technology, innovation, and cybersecurity and Internet policy. Previously, she served as chief of staff and lead science and engineering technical adviser as a contractor for the Defense Advanced Research Projects Agency (DARPA) foundational cyber warfare program, Plan X. Before DARPA, Ms. Zheng was director for global government relations and cybersecurity policy at CA Technologies, a \$5 billion enterprise software company, where she advised company executives on cybersecurity, data security and breach notification, and software assurance. While at CA, Ms. Zheng was a member of the Information Technology (IT) Sector Coordinating Council, IT Information Sharing and Analysis Center, SAFECode, and vice chair of the TechAmerica Cybersecurity Legislative Subcommittee.

Prior to CA Technologies, Ms. Zheng served as a professional staff member for the Senate Homeland Security and Governmental Affairs Committee. While in this role, she was a principal in drafting and negotiations for the Cybersecurity Act of 2012 and conducted oversight of critical infrastructure protection programs, spectrum auctions, privacy, and federal IT programs. Ms. Zheng previously held various positions at CSIS, including program manager of the Technology and Public Policy Program, where she managed the CSIS Cybersecurity Commission among other program initiatives. She has authored reports on U.S.-China relations and soft power, and civil space policy issues. Ms. Zheng holds a B.A. in economics and political science from the University of Michigan, studied government at the London School of Economics and Political Science, and completed graduate coursework in security studies at the Johns Hopkins University School of Advanced International Studies.

James A. Lewis is a senior fellow and program director at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His government experience includes work on Asian politico-military issues, as a negotiator on conventional arms and technology transfers, and on military and intelligence-related technologies. Lewis led the U.S. delegation to the Wassenaar Arrangement Experts Group on advanced civil and military technologies and was the rapporteur for the UN Group of Government Experts on Information Security for their successful 2010 and 2013 sessions. He was assigned to U.S. Southern Command for Operation Just Cause, U.S. Central Command for Operation Desert Shield, and to the U.S. Central American Task Force.

Since coming to CSIS, Lewis has authored numerous publications. His recent work focuses on cybersecurity, including the “Cybersecurity for the 44th Presidency,” which was commended by President Obama. He is an internationally recognized expert, and

his comments appear frequently in the media. Lewis has a close research partnership with the China Institutes of Contemporary International Relations. His current research examines sovereignty on the Internet, cybersecurity norms, warfare, and technological innovation. Lewis received his Ph.D. from the University of Chicago.

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202-887-0200 | www.csis.org