Bloomberg BNA

Privacy and Security Law Report®

Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns?

By Kimberly Peretti

On May 27, a well-known leader of several prominent hacktivist groups received a time-served sentence of seven months imprisonment even though he faced over 20 years under the federal sentencing guidelines. The primary reason for the reduction was his significant and complex cooperation with federal law enforcement authorities, which involved, among other things, convincing hackers to provide him with information regarding pending attacks. With this information, authorities were able to disrupt or prevent at least 300 separate computer hacks, including an attack on a critical infrastructure water utility in a U.S. city.[1]

While private companies and the government cannot expect to rely entirely, or even partially, on information provided by criminals for advanced warning of imminent cyber threats, a vast network of groups, platforms and methods is developing within industries and the government to identify and provide ''actionable'' cyber threat intelligence to companies. Indeed, companies that do not engage in such information sharing in the age of targeted cybercrimes committed by advanced—even state-sponsored—threat actors will find it increasingly difficult to mitigate the growing threat of exploitation, disruption and even destruction of their networks and systems.

This new age of cybercrime has ushered in with it a need for companies to work with various arms of the government that are involved in investigating cybercrime, protecting critical infrastructure or regulating data security practices. This multi-faceted and purposeful government involvement means that companies may be working with government officials with very different agendas, be it to investigate a criminal, identify systemic risk to an industry, protect consumers' personal information or ensure shareholders are properly informed about cyber risk. Indeed, the results of these government inquiries and investigations can be extremely favorable for the company (for example, information allowing immediate containment of an ongoing cyberattack) or extremely unfavorable (a 20-year agreement with the Federal Trade Commission (FTC) to refrain from certain data security practices). This dichotomy has particular relevance as companies consider embarking into information sharing both within the private sector and with the government.

This article will: (1) discuss the importance of exchanging cyber threat information; (2) identify various methods available to companies to share and receive cyber threat information; (3) delineate the categories of cyber threat information; (4) discuss the concerns with information sharing; and (5) provide guidance for companies to mitigate potential risks with information sharing.

I. Why Is Information Sharing Important for My Organization?

Simply put, information sharing is important for a combination of three reasons: (1) the receipt of critical threat data can and has been shown to prevent potential cyberattacks and mitigate ongoing attacks; (2) relying on compliance-based information security strategies alone does not adequately protect organizations against increasingly sophisticated attacks by increasingly sophisticated threat actors; and (3) criminals collaborate to perpetrate cybercrimes, and so companies and the government should also collaborate to reduce

[1] Government's sentencing statement at 11, *United States v. Monsegur*, No. 11 Cr. 666 (LAP) (S.D.N.Y. May 23, 2014), *available at* http://www.wired.com/wp-content/uploads/2014/05/Monsegur.pdf.

Kimberly Peretti is a partner at Alston & Bird LLP in Washington. She is a member of the firm's White Collar Crime Group and co-chair of the Security Incident Management & Response Team.

Lou Dennig, an associate in Alston & Bird's Litigation & Trial Practice Group and Security Incident Management & Response Team in Washington, contributed to the article.

 ISSN 1538-3423

the overall effectiveness of the criminals' far-too-successful pursuits.

As companies struggle to understand what steps they should take to address the ever-increasing risk exposure from cybersecurity incidents, information sharing is seen as a valuable part of the mix.[2] According to a recent study from PricewaterhouseCoopers LLP, 82 percent of companies that have ''high-performing security practices collaborate with others to deepen their knowledge of security and threat trends.''[3] In addition, leading cybercrime analysts recognize that ''public-private cyber information sharing can bolster and speed identification and detection of threats and will be critical to a coordinated response to a cyber incident.''[4] Working information technology security professionals also see the practical value of information sharing—in a recent study of 701 practitioners, 61 percent of respondents believed that ''exchanging threat intelligence . . . could have prevented their organization from experiencing a cyberattack in the past 24 months.''[5]

Information sharing is also a cost-effective tool in combating cybercrime. The Armed Forces Communications and Electronics Association Cyber Committee recently released a study on the economics of cybersecurity where it identified certain ''investment principles'' for companies to use in developing data security programs.[6] One such principle was that ''the economic benefit of participating in multiple, high quality cyber security information sharing exchanges regarding the dynamic characteristics of sophisticated threats is very high.''[7] The study also highlighted that a primary benefit of information sharing is the early identification and termination, or entire prevention, of cyberattacks. Because cyberattacks can lead to significant economic damage and reputational harm, the return on investment from stopping such an attack is significant.[8]

A. Methods of Information Sharing

Information security professionals have long relied on informal and semi-structured sharing networks and relationships with individuals in peer organizations to gain better insight into cybersecurity threats and vulnerabilities. A recent study on information sharing shows that such networks are alive and well as it identified that the most common source of threat intelligence, with a 58 percent response rate, was ''peers in other companies'' as opposed to industry associations or other entities.[9] Additionally, a common method of information sharing is through informal mechanisms, as 54 percent of respondents said that they commonly received threat intelligence through ''peer group discussion via phone, e-mail or in-person.''[10]

A separate method of information sharing can be defined as ''post-to-all'' models, which are similar to Listservs where organizations can post information regarding a cybersecurity incident to a message board or send out an e-mail to a large group. While ''post-to-all'' models offer a low-cost and efficient method of distributing information, the recipients must often take the added step of analyzing the data to identify how it may affect their system.[11] Indeed, many entities embarking down the information-sharing path complain that the volume of information received—and required resources to sift through the data—outweighs any potential benefits that may be derived by the receipt of such data.[12] To address these concerns, certain business sectors have pooled their resources to create, or have simply joined existing, Information Sharing and Analysis Centers (ISACs), which are designed to streamline the collection, analysis and dissemination of threat intelligence within a given sector.

ISACs developed as a more formal information-sharing mechanisms primarily in response to Sept. 11, 2001.[13] Critical infrastructure sectors (such as banking,

[2] In recent congressional testimony, the National Retail Federation (NRF) recognized that a ''critical aspect of next generation information security is the ability to share and receive actionable threat intelligence in a timely manner . . . . By working together with government to disseminate and receive cyber threat information, companies can learn where to look for signs of an attack and how to alter their security systems to 'plug holes' and block attempted intrusions carried out using techniques that were effective in earlier attacks.'' Testimony of Tom Litchford before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, *Protecting Your Personal Data: How Law Enforcement Works With the Private Sector to Prevent Cybercrime* (Apr. 16, 2014).

[3] *See* PricewaterhouseCoopers LLP, *U.S. Cybercrime: Rising risks, reduced readiness 2014* (June 2014), *available at* http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf (citing PwC, *CSO* magazine, *CIO* magazine, *The Global State of Information Security Survey 2014* (Sept. 2014)).

[4] Bipartisan Policy Center, National Security Program, *Cyber security Task Force: Public-Private Information Sharing* (July 2012), *available at* http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf.

[5] Ponemon Institute, *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way* (Apr. 2014).

[6] *See* Armed Forces Communications and Electronics Association Cyber Committee, *The Economics of Cybersecurity Part II: Extending the Cybersecurity Framework* (Apr. 2014), *available at* http://www.afcea.org/committees/cyber/documents/EconomicsofCybersecurityPartII-Final4-2-14.pdf (relying on a cybersecurity model developed by Robert Lentz, former director of cybersecurity for the Department of Defense (DOD), which ''predicted the economic benefits of security countermeasures for addressing sophisticated threats, referred to in the model as Advanced Persistent Threats (APT) and Nation State threats. Specifically, Lentz's model recommended ways to reduce overall cost to an organization in addressing sophisticated threats'').

[7] *Id.*

[8] *Id.*

[9] *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way supra* note 5.

[10] *See id.* (asking IT professionals to identify their primary sources of threat intelligence and finding that both formal and informal sharing methods are widely used. In terms of formal sharing, 26 percent received intelligence from industry associations, such as Information Sharing and Analysis Centers (ISACs), 33 percent from law enforcement entities and 55 percent from for-profit IT security vendors).

[11] David Inserra and Paul Rosenzweig, *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, The Heritage Foundation Backgrounder No. 2899 (Apr. 1, 2014), *available at* http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

[12] *Cyber security Task Force: Public-Private Information Sharing*, *supra* note 4.

[13] *See Testimony of Gregory T. Garcia on Behalf of FS-ISAC* (Mar. 5, 2014), *available at* http://financialservices.house.gov/uploadedfiles/hhrg-113-ba15-wstate-ggarcia-20140305.pdf.

   ISSN 1538-3423

energy and telecommunications), and increasingly other sectors,[14] have developed ISACs to more efficiently leverage cyber threat data. ISACs follow a ''hub-and-spoke'' model where companies send cyber threat data to a common entity or ''hub'' that in turn organizes and analyzes the data before sending actionable threat intelligence out to ISAC members.[15] One benefit of the ISAC model is that it creates trusted entities that private sector organizations can become increasingly comfortable with over time, and with which the government is more willing to collaborate, thereby facilitating additional information sharing.[16]

Exemplifying the ideal version of this model is the Financial Services ISAC (FS-ISAC), which was created in response to a 1998 presidential directive designed to facilitate cooperation between the public and private sectors in combating cyber threats to U.S. critical infrastructure.[17] The FS-ISAC has been hailed as the gold standard of effective information-sharing mechanisms, a status buttressed by its close collaboration with the U.S. government agencies primarily responsible for combating cyber threats, including the Department of Treasury, the Department of Homeland Security (DHS) and the Secret Service.[18] Its effectiveness was highlighted during a series of unprecedented distributed denial-of-service (DDoS) attacks last year on the financial services sector, where it was instrumental in mitigating the impact of the attacks.[19] The FS-ISAC was able to quickly analyze received threat information from any particular institution under attack and push out relevant and actionable information in near real-time to other institutions, thus allowing those institutions to take measures to significantly mitigate imminent attacks on their systems.[20]

The cyber threat has not abated, and recently the need for established methods of direct government-to-private-sector and private-sector–to-government sharing has been highlighted. Signaling the importance of the issue, in 2013, President Barack Obama unveiled an executive order (EO) designed to improve the cybersecurity of critical infrastructure entities and stressed the need for improved information sharing.[21] A stated goal of the EO is for the government to increase ''the volume, timeliness, and quality'' of the threat data it shares with the private sector so those entities may better protect themselves from attacks.[22] To enhance the government's ability to share information both internally and with the private sector, in 2009 DHS created the National Cybersecurity & Communications Integration Center (NCCIC), which essentially functions as a fusion center for the entire federal government as well as state and local governments. As a central hub for the government's cyber threat intelligence, the NCCIC's collaboration with ISACs allows the private sector to have better situational awareness regarding potential threats, and more quickly respond to and recover from security incidents that it learns of from the government. Indeed, following the pronouncements of the EO, the NCCIC has increased its visibility and activity, filling a much needed void by creating a primary touch point for the private sector to share and receive cyber threat intelligence.

Further, the U.S. government is taking specific steps to remove perceived barriers to cyber threat information sharing, as discussed in section II, *infra*.

B. Type of Information Shared

Information-sharing programs are designed to distribute ''actionable threat intelligence,''[23] or in laymen's terms, technical data that an organization's information security team can use to prevent, detect or block an attack. The core of that threat intelligence is what is referred to as TTPs or ''Tactics, Techniques and Procedures.''[24] TTPs are the behavior and *modus operandi* of cybercriminals that shed light on how they compromise and exploit systems. Using malware to steal credit card information is a tactic, and the technique related to that tactic could be sending an e-mail containing malicious code that, once opened, captured keystrokes to identify and steal credit card numbers. A procedure related to such an attack could be registering a domain for the purpose of creating an e-mail account that could circumvent antivirus protections and spam blockers.[25] TTPs include not only information related to a cybercriminal's attack pattern, but also the tools they use to carry out attacks, specific technical data on the malware they use (*e.g.*, name, hash values), information on the type of victim they target (*e.g.*, type of company,

[14] Academia has developed the Research and Education Networking ISAC (REN-ISAC), the mission of which is to promote the cybersecurity operational protection within the higher education and research communities. *See* http://www.ren-isac.net/. Additionally, the National Retail Federation (NRF) is in the process of developing an ISAC for the retail industry. *See* Press Release, NRF, National Retail Federation Announces Information-Sharing Platform, (Apr. 14, 2014), *available at* https://nrf.com/media/press-releases/national-retail-federation-announces-information-sharing-platform.

[15] *Cybersecurity Information Sharing*, *supra* note 11.

[16] *Cyber security Task Force: Public-Private Information Sharing*, *supra* note 4.

[17] *See Testimony of Gregory T. Garcia* , *supra* note 13 (noting that after 9/11 FS-ISAC expanded to collect and disseminate not only cyber threat information, but also physical threat data. This expansion into physical threat data was also in response to Homeland Security Presidential Directive 7, Presidential Policy Directive 21 and the Homeland Security Act.).

[18] *Id.*

[19] Tracy Kitten, *DDoS: Lessons from Phase 2 Attacks*, Bank Info Security, Jan. 14, 2013, *available at* http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1.

[20] *Id.*

[21] Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,741 (Feb. 12, 2013) (12 PVLR 257, 2/18/13).

[22] *Id.*

[23] Other commonly used phrases include ''cyber threat intelligence,'' ''cybersecurity threat indicators,'' ''cyber threat information,'' ''cyber information sharing'' and ''cyber threat intelligence exchange.''

[24] *See* Sean Barnum, The MITRE Corporation, *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)*, Version 1.1, Revision 1 (Feb. 20, 2014), *available at* http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf (providing an overview of Structured Threat Information eXpression (STIX), which is a DHS-sponsored initiative to provide a common format for cyber threat information sharing to encourage more efficient and easier sharing. DHS and NCCIC both utilize STIX for some of their programs, and in 2012 FS-ISAC announced that it would use the STIX architecture for its cyber threat information sharing).

[25] *Id.*

geographic sphere, demographic data on targets) and the Internet protocol (IP) addresses used to attack a company's system or the IP addresses programmed to receive commands or data from compromised systems within a company's environment.[26] TTPs play a central role in the type of ''actionable threat intelligence'' that information-sharing programs are designed to leverage so that companies can prepare themselves to detect and defend against attacks.[27]

II. What Are the Concerns With Information Sharing?

While an increasing number of companies are recognizing the benefits of sharing information regarding cyber threats, many remain wary because of concern that: (1) disclosure of cyber threat information may conflict with legal obligations concerning the protection of personal information; (2) information sharing could raise antitrust concerns leading to government action; (3) confidential information could be discoverable through a Freedom of Information Act (FOIA) request; and (4) cyber threat information exchange could lead to regulatory action or civil liability. While some of these concerns are more theoretical than actual, and some have been alleviated by recent government measures, companies should understand any potential risks associated with exchanging cyber threat information and take steps to mitigate such risks in order to take advantage of the very real benefits that the receipt of cyber threat data can bring.

A. Violations of Legal Obligations Related to Privacy Protections

A variety of state and federal privacy laws govern the collection, storage, use and disclosure of various types of personal, sensitive or otherwise regulated information. Under most circumstances, actionable threat information, as described in the previous section, does not include, or need to include, the type of privacy-related information that companies are hesitant to disclose, such as data elements that may constitute ''personal information'' under such federal or state statutes. And, any such information (*e.g.*, e-mail addresses, credit card numbers) can often be redacted, withheld or removed without undermining the sharing process. As aptly stated in one report:

> While sensitive and personal data on e-mails and in databases may be the target of cyberattacks, 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, [the focus is on] sharing information about threats, vulnerabilities, and IP data.[28]

While privacy concerns should not be minimized or ignored, companies should understand the alternatives available to a request that appears to raise these concerns, take steps to ensure personal information is not shared as appropriate[29] and push back on any potential recipient requesting a broad information set that may include personal information.

Internet service providers and other hosting companies have also expressed concerns that sharing certain types of cyber threat information may violate federal privacy laws governing the disclosure of customer information. Under the Stored Communications Act (SCA), communications service providers are generally prohibited from disclosing customer information to outside parties, including the government.[30] As leading analysts remarked, a broad interpretation of customer information ''could be and is being construed by many to include the coding of viruses and malware and the IP addresses from which cyberattacks [against their customers] are originating.''[31] Under such an interpretation, for those entities subject to the SCA sharing the cyber threat data through an information-sharing platform could potentially violate the act.

To alleviate these concerns, in May 2014, the Department of Justice (DOJ) released a white paper outlining its interpretation of how cybersecurity information sharing interacts with the SCA.[32] According to the DOJ, communications companies are permitted to disclose ''non-content information to the government'' as long as that information is in its ''aggregate form,'' meaning it cannot be ascribed to a single customer.[33] The DOJ provided examples of cyber information that can be shared, noting that ''characteristics of a computer virus or malicious cyber tool that do not divulge subscriber or customer-specific information (*e.g.*, the associated file

---

[26] *Id.*

[27] For example, the Cybersecurity Information Sharing Act of 2014 (S. 2588) (introduced by Sen. Dianne Feinstein (D.-Calif.) July 10) would create an information-sharing program designed to encourage the flow of ''cyber threat indicators'' between the private sector and the government. The bill defines the term ''cyber threat indicator'' as: ''information that is necessary to indicate, describe or identify— (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (B) a method of defeating a security control or exploitation of a security vulnerability; (C) a security vulnerability; (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (E) malicious cyber command and control; (F) the actual or potential harm caused by an incident, including information exfiltrated when it is necessary in order to describe a cybersecurity threat; (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (H) any combination thereof.'' The full text of the bill is available at https://beta.congress.gov/113/bills/s2588/BILLS-113s2588pcs.pdf (13 PVLR 1231, 7/14/14).

[28] *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, *supra* note 11.

[29] In addition to privacy laws and regulations that may come into play with the disclosure of personal information, a company's privacy policies and customer contracts may address whether, and under what circumstances, personal information may be shared with the government. Companies need to ensure that their information-sharing practices comply with any restrictions or statements in consumer, customer or employee agreements, contracts or policies.

[30] 18 U.S.C. § 2701 *et seq*.

[31] *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, *supra* note 11.

[32] DOJ White Paper, *Sharing Cyberthreat Information Under 18 U.S.C. § 2702(a)(3)* (May 9, 2014), *available at* http://www.justice.gov/criminal/cybercrime/docs/guidance-for-ecpa-issue-5-9-2014.pdf.

[33] *Id.*

  PVLR ISSN 1538-3423

size, protocol or port) could be shared.''[34] In addition, ''Internet traffic patterns'' may be shared as they do not require disclosure of customer information.[35]

B. Antitrust Concerns

Companies have expressed concern that sharing information regarding cyber threats could be interpreted by government regulators as anti-competitive behavior.[36] In fact, 26 percent of IT professionals identified ''Anti-competitive concerns'' as one of the three primary reasons for not participating in information-sharing programs.[37] Similar to its response to SCA privacy law concerns, in April 2014, the DOJ, in conjunction with the FTC, issued a policy statement clarifying the extent to which cyber threat information sharing could raise antitrust issues.[38] The agencies underscored that their real concern was the sharing of competitively sensitive information such as ''current, and future prices, cost data, or output levels'' that could allow for ''competitive coordination among competitors.''[39] Their policy statement recognized that the type of technical data shared in information programs is generally unrelated to the competitively sensitive information about which the agencies are concerned. As such, the agencies announced that as long as information-sharing mechanisms were properly designed to share threat information as opposed to competitively sensitive information, such sharing ''is not likely to raise antitrust concerns.''[40]

The release of the SCA white paper and joint DOJ/FTC policy statement demonstrates the government's intent to take steps to remove perceived barriers to information sharing and help the private sector achieve a greater level of comfort when providing threat data to federal agencies.

C. Confidential Information Revealed Through FOIA Requests

One of the primary concerns expressed about information sharing is that ''private proprietary information compiled in government databases will be discoverable through FOIA requests.''[41] FOIA protection remains such an important issue that all of the recently proposed cybersecurity legislative initiatives included language protecting cyber threat information shared with the government from disclosure through FOIA requests.[42]

Congress and DHS have taken certain steps to address this concern by creating the Protected Critical Infrastructure Information (PCII) Program, which grants broad statutory protection to certain cyber threat data shared with DHS.[43] The PCII Program protections are derived from the Critical Infrastructure Information Act of 2002 (CIIA), which is part of the Homeland Security Act.[44] When companies share critical infrastructure information with DHS,[45] and DHS determines that the submitted information meets the required definition, both the information and the identity of the submitting entity is exempt from not only FOIA requests, but also from any state, tribal or local disclosure laws.[46]

However, there are several limitations to the usefulness of the PCII Program for broader private sector-to-government cyber threat information sharing. First and self-evident, the protections are only applicable to data related to critical infrastructure entities, rather than threats to all sectors.[47] Second, it is unclear whether all types (or the most common types) of actionable cyber threat intelligence constitute ''critical infrastructure information,'' despite the regulation's seemingly broad definition of the term.[48] And third, the actual threat data may only be shared with DHS and other authorized government actors as part of, and under the umbrella of, the PCII Program.[49] This means that, instead

---

[34] *Id.*

[35] *Id.*

[36] *Cyber security Task Force: Public-Private Information Sharing*, *supra* note 4.

[37] *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way*, *supra* note 5.

[38] DOJ & FTC, *Antitrust Policy Statement on Sharing of Cybersecurity Information* (Apr. 10, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf (13 PVLR 653, 4/14/14).

[39] *Id.*

[40] *Id.*

[41] *Cyber security Task Force: Public-Private Information Sharing*, *supra* note 4.

[42] *See* Rob Strayer & David Bearwood, National Security Program, Homeland Security Project, *Cybersecurity Legislation Privacy Protections are Substantially Similar* (July 2, 2012), *available at* http://bipartisanpolicy.org/sites/default/files/Cyber%20Privacy%20Paper.pdf (noting that the Cyber Intelligence Sharing and Protection Act (CISPA) (H.R. 3253), Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act (SECURE IT Act) (S. 3342) and Cybersecurity Act of 2012 (S. 2105) all included provisions protecting cyber threat information shared with the government from FOIA requests).

[43] 6 C.F.R. §§ 29.1–29.9. For an overview of the PCII Program, see the DHS Web page available at http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program.

[44] 6 U.S.C. § 133(a)(A).

[45] *See* 6 U.S.C. § 131(3) (defining ''critical infrastructure information'' subject to protection as information that is either (1) ''not customarily in the public domain'' and deals with an ''actual, potential or threatened interference with, attack on, compromise of or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack,'' (2) deals with ''the ability of any critical infrastructure or protected system to resist such interference, compromise'' or attack'' or (3) ''any planned or past operational problem or solution regarding critical infrastructure or protected systems''). DHS is responsible for determining whether submitted critical infrastructure information meets the definition and as such is granted statutory protection. 6 C.F.R. § 29.6(a). If information is deemed *not* to meet the definition, it must either be returned to the submitter, or must be destroyed. *Id.* § 29.6(e)(ii).

[46] Data shared through the PCII Program may only be viewed by federal, state or local government personnel or contractors who are granted specific authorization to view such data and are trained in its proper handling. 6 C.F.R. § 29.8(b). Contractors must also sign nondisclosure agreements to view such information. *Id.* § 29.8(c). Anyone found to have improperly disclosed such data is subject to loss of their security clearance (and with it, likely their job) as well as fines and possible imprisonment. *Id.* § 29.9(d).

[47] 6 U.S.C. § 131(3).

[48] 6 U.S.C.A. § 131(3).

[49] 6 U.S.C. § 131(3). While other government agencies have taken some steps to protect shared cyber threat data, DHS has the most robust protections in place. For example, the DOD issued a final rule stating that it would protect the confidentiality of sensitive cyber threat information ''to the maximum extent authorized by law, regulation and policy'' including using any applicable exemptions under FOIA or the Privacy Act.

of sharing directly with arms of DHS (such as the NCCIC and the United States Computer Emergency Readiness Team (US-CERT)) responsible for collecting and analyzing cyber threat data, in order to take advantage of the statutory FOIA protections companies have to avail themselves of the PCII Program, and ensure (working with DHS) that the information to be shared meets the requirements of the program. These steps necessarily add an extra layer of process that may be sufficient to ultimately defeat the purpose of near real-time information sharing. Nonetheless, information shared through the PCII Program is useful as it can be sanitized and used by the NCCIC and US-CERT to prepare advisories, alerts and warnings for disclosure to specific companies, targeted sectors or other government entities.[50] In this way, if the PCII Program could be expanded to include a broader range of cyber threat data and a broader set of government recipients, and incorporate a streamlined sharing process, one could imagine that it could provide a strong model for the type of protection needed to encourage robust information sharing.

D. Lack of Protection From Regulatory Action or Civil Liability

Without safe harbor or liability protections related to information shared both among private sector actors and with the government, companies are concerned that information sharing will lead to action from regulators, civil lawsuits or both.[51] Cybersecurity experts have repeatedly stressed that the lack of protection from liability is a primary hindrance to information sharing.[52]

The concern that regulators will use shared information to investigate and potentially take action against a company is of particular concern given the regulators' responsibility and/or interest in assessing companies' data security practices, both before and after a breach. In the early stages of an investigation involving a security incident, entities are likely to be working with—and sharing information with—law enforcement and potentially private sector ISACs. Indeed, it is in these early stages that sharing information—if it is to have any value—must occur. As the investigation progresses, a company's security breach may become public through a required notification to customers, a public filing or merely being named as a victim in an indictment.[53] When this happens, particularly if the incident involves personal or regulated data, the company can expect to receive an inquiry from a federal or state regulator, or both, scrutinizing the company's disclosure with respect to the incident and/or the company's underlying information security practices. In fact, regulators often request that a company provide them with the same information that the company shared with law enforcement as part of law enforcement's criminal investigation.

Companies experiencing a data breach can also expect plaintiffs to sue under a myriad of legal theories, including negligence, breach of express or implied contract, state deceptive trade practices act violations or state data breach notification violations, among other claims. Such information shared with the government or other parties, particularly the timing of when the incident occurred and the company's knowledge thereof and the controls in place (or lacking) at the time of breach, may be used unfavorably against the company by the regulators or class action plaintiffs.

III. Guidance for Companies to Engage in Information Sharing

Congress is keenly aware of the importance of protecting companies from liability for information-sharing activities as recent cybersecurity legislative proposals, as well the Cybersecurity Information Sharing Act introduced in June of this year by Sen. Dianne Feinstein (D-Calif.), have all included broad liability protections.[54] Enshrining such protections in statutes could certainly remove the remaining perceived and actual barriers for companies to engage in robust cyber threat information sharing. While the debate ensues, however, companies need to take steps to engage in information sharing as it is an important weapon against the cyber adversary that companies cannot afford to be without. In doing so, companies should keep the following guidance in mind to ensure they appropriately mitigate the concerns delineated above.

Protect Your Privilege: It is important for companies to remember that they must take steps to maintain privilege protections. One of the primary benefits of engaging outside counsel at an early stage of a data breach investigation is that it protects certain communications and information from disclosure. Privilege protections are unlikely to be affected when companies share the type of technical data that are most beneficial

---

DOD, Defense Industrial Base Voluntary Cyber Security and Information Assurance Activities, 32 C.F.R. pt. 236 (12 PVLR 1828, 10/28/13).

[50] 6 C.F.R. § 29.8(e); http://www.us-cert.gov/about-us. *See* DHS, *National Cyber Incident Response Plan* 18 (Sept. 2010), *available at* http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf (noting that NCCIC has processes in place for receiving PCII Program information).

[51] *See Exchanging Cyber Threat Intelligence: There Has to Be a Better Way*, *supra* note 5 (showing that 50 percent of respondents see potential liability from information sharing as one of the primary reasons their companies do not engage in more robust information sharing).

[52] *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, *supra* note 11 (finding the ''current lack of protection is one of the biggest obstacles to information sharing, as evidenced by many companies' and trade organizations' statements'').

[53] For example, recently, three U.S. public companies were among the victims named in the first-ever criminal indictment of state-sponsored actors for cyber espionage activities. Press Release, DOJ, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, (May 19, 2014), available at http://www.justice.gov/opa/pr/2014/May/14-ag-528.html (13 PVLR 905, 5/26/14). After the DOJ indicted several Chinese officials for carrying out the attacks, which involved the theft of trade secrets and other data, the companies found themselves receiving (media) scrutiny for not previously disclosing the cyber attacks to investors in Securities and Exchange Commission filings. Chris Strohm, Dave Michaels, & Sonja Elmquist, *Chinese Hacking Raises Cyber Attack Disclosure Issue for Companies*, Insurance Journal, May 21, 2014, *available at* http://www.insurancejournal.com/news/national/2014/05/21/329707.htm.

[54] David McAfee, *Sen. Introduces Draft of Cybersecurity Data Sharing Bill*, Law360, *available at* http://www.law360.com/articles/548976/sen-introduces-draft-of-cybersecurity-data-sharing-bill.

  PVLR ISSN 1538-3423

for the information-sharing community. And, privilege is a valuable tool in minimizing the risk exposure from regulatory inquiries and civil actions following the disclosure of a security incident.

A. Guidance Specific to Sharing Information With Government Agencies

Review Data Requests to Understand Your Protections: Data shared with the government can potentially be protected from disclosure or use in civil litigation based on the law and regulations that apply to the agency making the request as well as potential protections in place due to the form of the request. For example, if a request for information from the DOJ is in the form of a grand jury subpoena seeking cyber incident information, a company can feel comfortable that information produced can be reasonably expected to remain confidential due to the substantial secrecy protections afforded information sought by a grand jury.[55] This information thus cannot be freely shared with other government agencies, such as the FTC, or be discoverable via a FOIA request. As a second example, information shared with DHS as part of the PCII Program is afforded certain protections, including not being disclosed through a FOIA request.[56] Additionally, data shared through the PCII Program cannot be used in a civil action against a company by a government agency, state or local authority or any third party as long as the data were shared in good faith.[57]

When Few Protections Exist—Ask for Them: Even when no clear authorities or protections exist, as with the bulk of cyber threat information requested by, or desired to be shared with, the government, companies should request a confidential and/or business sensitive FOIA exemption, and push agencies to provide oral (or preferably written) confirmation that such information will not be further disclosed or shared with other government branches or agencies beyond the purpose for which it is submitted. Given this administration's focus on promoting mechanisms to facilitate private sector to public sector information sharing, it is not unreasonable to expect such confirmations from agencies seeking the receipt of such data.

Don't Let Agencies Punish Your Good (Sharing) Deeds: If a situation arises where an interested regulator requests cyber threat data the company previously shared with another arm of the government in an effort to aid that other agency's mission (*e.g.*, to help solve a crime or assist in identifying a systemic risk to an industry) the company should provide pushback. This administration has been clear that its goal is to create a robust information-sharing environment between the public and private sector. Attempts by regulators to use shared information to investigate and potentially initiate enforcement action against a company run counter to the spirit of the administration's push for broad collaboration.

B. Guidance Specific to Sharing Information With the Private Sector

Have a Share-First Mentality With Established Entities: Engaging in information sharing through ISACs or Listservs that have defined operating rules brings minimal risks (*e.g.*, private companies are not subject to FOIA), is a low-cost data security measure and the information received can help prevent costly, image-damaging cyberattacks.

Share Smart and Worry Less: Take advantage of options offered by ISACs and other mechanisms, such as anonymity protections, to assuage concerns regarding sharing. Additionally, mitigate concerns with privacy issues by sharing only the type of technical, actionable threat intelligence that is truly useful to other entities.

Know Your Company's Sharing—Identify Current Informal Mechanisms: A corporation's legal team should make an effort to understand any informal information sharing that is already conducted by their information security personnel in order to identify any potential risks or needed protections with the current structure, as well as identify any additional information-sharing networks that may be of value to the enterprise.

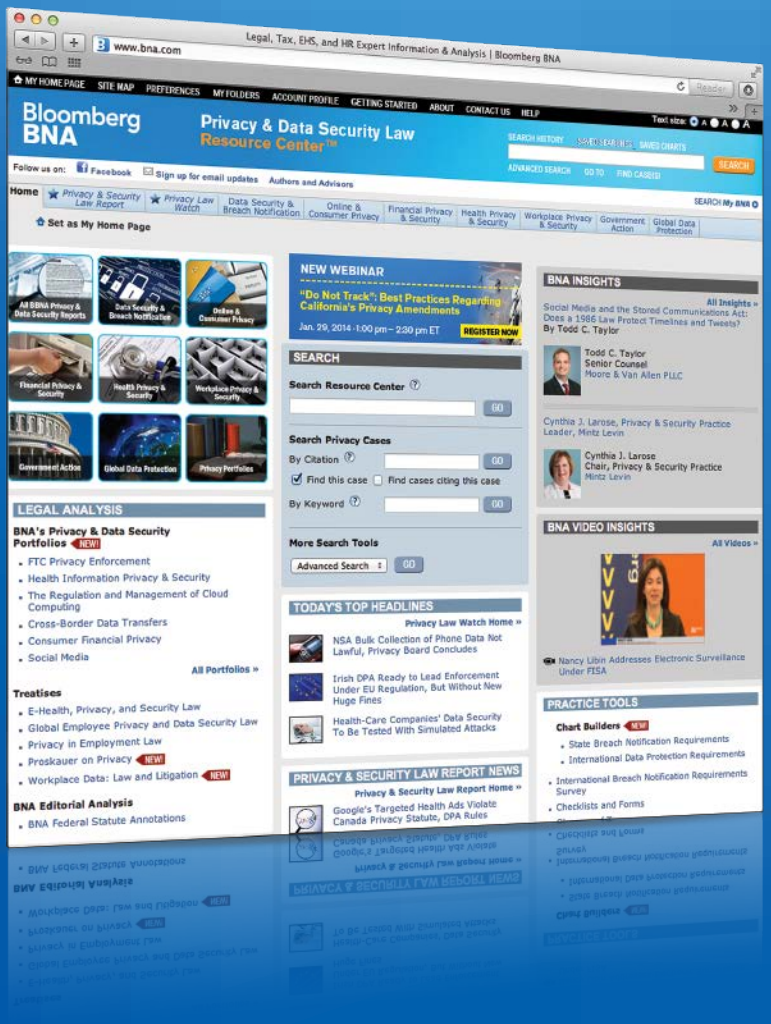
Information sharing is a crucial tool in a company's fight against cybercrime, but until liability protections are ensured by statute it is an area that requires creative solutions for additional layers of protection.

---

[55] Fed. R. Crim. P. 6(e).
[56] 6 U.S.C. § 133(a)(A).
[57] *Id.* § 133(a)(C).

NEW PORTFOLIOS & TREATISES NOW AVAILABLE

SAFE DATA & SOUND SOLUTIONS



Privacy & Data Security Law Resource Center™

Unparalleled news. Expert analysis from the new Privacy & Data Security Portfolio Practice Series. Comprehensive new treatises. Proprietary practice tools. State, federal, and international primary sources. The all-in-one research solution that today's professionals trust to navigate and stay in compliance with the maze of evolving privacy and data security laws.

TO START YOUR FREE TRIAL CALL 800.372.1033 OR GO TO www.bna.com/privacy-insights

Bloomberg BNA