KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org
CENTER FOR DEMOCRACY & TECHNOLOGY

The Technical Gap in Information Sharing Policy

IAB/ISOC Workshop Coordinating Attack Response at Internet Scale (CARIS)
Joseph Lorenzo Hall (joe@cdt.org)
1 May 2015

I. Information Sharing Policy in the United States

Information sharing policy is a hot topic in legislative and regulatory forums, with no less than three US Congressional bills[1] (at the time of submission) that would extend broad liability protection to private firms that share information to respond to computer and network security attacks (referred to as "cybersecurity" in Washington, DC). This represents a massive sea change in how network and service operators may operate in the future, where they exchange broad immunity from liability – from even the most stringent legal protections – for increased sharing of information with other private firms and with the government. For example, the US wiretapping statutes prohibit both intercepting communications (without an operational need for network management) and disseminating those intercepted communications externally; effectively prohibiting sharing communications contents.

However, there is clearly a gap in understanding between what is needed for incident response and what is needed for forensic investigation. The leading bill in the US Senate, the Cybersecurity Information Sharing Act (CISA), allows sharing between firms and with the government of what the bill defines as "cyber threat indicators," which is not a standard technical term. The definition, included below, is exceedingly broad:

> CYBER THREAT INDICATOR.–The term ''cyber threat indicator'' means information that is necessary to 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;

[1] These bills include: the Cybersecurity Information Sharing Act (CISA) [https://www.congress.gov/114/bills/s754/BILLS-114s754pcs.pdf] in the US Senate, and in the US House of Representatives, the Protecting Cyber Networks Act (PCNA) [http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HR1560.pdf] and the National Cybersecurity Protection Advancement Act of 2015 [http://www.scribd.com/doc/259428604/National-Cybersecurity-Protection-Advancement-Act-Draft-3-20-15].

> (C) a security vulnerability, including anomalous activity that appears to indicate the existence of 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

A cybersecurity threat is defined in CISA as:

> An action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system, but not an action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

The elements of the above definition of a "cyber threat indicator" are very broad and essentially a grab bag of both mitigation-related information and forensic information. That is, it includes elements that look like information shared as Indicators of Compromise (IOCs), including attack and malware signatures as well as elements/tuples for whitelists/blacklists and evidence of social engineering like phishing campaigns. However, it also includes information needed for forensic/after-action investigation of an attack, such as exfiltrated data and anomalous network patterns suggesting malicious reconnaissance. (As a third category, it does seem to include things that have no real technical analog by name such as "malicious cyber command and control" which could be C&C protocol elements, botnet network structure graphs or potentially anything conceivably thought to be related to distributed attack structures.)

II. Information Sharing Policy in the EU

Information sharing policy seems to be not as well developed in the EU and elsewhere. There is significant discussion about requirements to notify EU member state authorities in the event of attacks or data breaches, but the information that would be shared is different than the classes of information I highlight above. That is, EU member states and cross-member coordinating bodies seem to want to know quickly the fact that an attack occurred and some relevant metadata about the attack, and that member state Data Protection Authorities (DPAs) are also notified with the same information in addition to a list of the people affected by an attack or breach.

One EU member state, France, appears to be exploring avenues of direct information sharing between industry and the government,[2] but specifically in an anti-terrorism context. In the wake of the massacre of satirical journalists earlier this year in France, French PM Valls introduced a new Intelligence Bill this past March. Among its provisions Article 2 of the bill allows the Prime Minister to require network operators and online content providers to install "black boxes" on their networks and services that are under the government's control to inspect network traffic in real time and, controversially, to potentially modify or otherwise interfere with network traffic. This compelled form of general information sharing, rather than voluntary incident-based information sharing is quite different than the policy developing in the United States. Notably, it appears that French PM Valls has decided to send this legislation to the French Constitutional Court given the public outcry that the introduction of this legislation sparked.

III. CDT's Interest

As a member of civil society, I may seem to be a strange fit for the CARIS workshop, since it focuses on "operators, researchers, CSIRT team members, service providers, vendors, [and] information sharing and analysis center members".[3] However, since these kinds of information sharing policy decisions are being made now and very quickly – in fact, it may be the case that the US Congress passes one or more of these bills and they may be signed into law by US President Obama before the CARIS workshop – it is critical that policymakers and stakeholders outside information sharing communities in the future have a better understanding of what is technically needed, precisely, to respond to attacks in a coordinated manner, at scale. Providing unbiased accessible technical input to policymakers and regulators is a major part of what I do.

I hope to do two things at the CARIS workshop: 1) understand better the international landscape for information sharing and what policies may drive, inhibit, or facilitate those activities; 2) explain the current state of the legislative and regulatory landscape to technical operators who may not be as active in the policy sphere, as well as CDT and civil society's concerns with unhindered sharing of forensic information free from liability – which inevitably includes personal and sensitive information; and, 3) understand better from the workshop participants what kinds of information are crucial to share amongst operators and with governments and any technical or process-related measures that are designed to narrowly tailor information to what is needed to respond to attacks in the short and medium term.

---

[2] Félix Tréguer, "France's Intelligence Bill: legalising mass surveillance," *Open Democracy* (29 April 2015), available at: https://www.opendemocracy.net/digitaliberties/félix-tréguer/france's-intelligence-bill-legalises-mass-surveillance.

[3] https://www.iab.org/2015/03/05/call-for-papers-iabisoc-workshop-on-coordinating-attack-response-at-internet-scale-caris/