Testimony

Sharing Information about Threats is not a Cybersecurity Panacea

Martin C. Libicki

RAND Office of External Affairs

CT-425

March 2015

Testimony presented before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on March 4, 2015

Published 2015 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Email: order@rand.org

Martin C. Libicki[1]
The RAND Corporation

Sharing Information about Threats is not a Cybersecurity Panacea[2]

Before the Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
House of Representatives

March 4, 2015

Good morning, Chairman Ratcliffe, Ranking Member Richmond, and distinguished members of the subcommittee. I thank you for the opportunity to testify today about the President's cybersecurity information-sharing proposal.

The President's initiatives to improve cybersecurity through information-sharing are laudable. Information-sharing can and should be an important element in efforts to ensure that defenders learn from each other faster than attackers learn from each other. The fact that attackers *do* learn from each other is something that we know from research that RAND conducted for a report released last year on cybercrime markets (*Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*).

People have been calling for greater information-sharing for almost 20 years, dating back to the formation of Information Sharing and Analysis Centers (ISACs) in the late 1990s and continuing through the recent reformulation of ISACs into Information Sharing and Analysis Organizations (ISAOs). Although more information *is* being shared, the President's initiatives are prompted by the perception that information-sharing is not advancing fast enough. Those asked to share gain little directly from sharing and believe they face financial, reputational, and legal risks in doing so. As a result, legislation has been repeatedly introduced to facilitate the increased exchange of information—notably, I would argue, *threat* information. Without going into a detailed assessment of the privacy implications of such legislation, apart from noting that concerns *have* been raised, its purposes are nevertheless sound and its passage can help improve cybersecurity.

Two concerns, however, merit note. One is that the current proposals do not address, and may even exacerbate, the differences between the cybersecurity enjoyed by small- and medium-sized

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/CT425.html.

enterprises on the one hand and that enjoyed by large enterprises on the other: a cybersecurity divide. The second concern is that the current legislative proposals represent an enormous amount of political energy dedicated to what is actually a narrowly focused point solution to the problem of cybersecurity when a much broader approach is required. Consider each concern in turn.

The cybersecurity divide exists roughly at the boundary between those organizations that are large enough to afford their own chief information security officer (CISO) and those that cannot. As a very rough estimate, though this varies by sector, organizations with more than one thousand employees can afford to hire a CISO, and those that are smaller cannot. Organizations that cannot afford to employ a CISO can usually offer only generalized cybersecurity training for their employees (if they do so at all); must rely on commodity hardware and software, often deployed with default settings; make do with commercial network offerings such as routers; and use off-the-shelf firewall tools. Organizations that can afford to employ a CISO can offer and customize specialized training, can afford to optimize their hardware and software for cybersecurity, can purchase sophisticated cybersecurity tools, can hire information security analysts, and contract with third parties for additional cybersecurity services. Fortunately, cloud offerings can be and are tailored for organizations of all sizes, but this only represents a partial approach to cybersecurity and may introduce a few additional security problems of their own.

ISAOs, laudable as they may be, are oriented toward organizations that can afford their membership fees; at $10,000 a year, most small- and medium-sized organizations are priced out of that market. Consider the likelihood that these ISAO's become the primary—or worse, exclusive—conduit for information-sharing between the government and private organizations. If so—and in the absence of other mechanisms to share information with the broader public—the smaller organizations are going to be left out. Whatever advantage they reap from information-sharing rests on the hope that the existence of ISAOs as conduits for shared information does not detract from paths more suited to smaller enterprises.

The risks of exacerbating the cybersecurity divide are related to the problem of an overly narrow focus for information-sharing associated with pending legislation.

Several weeks ago, during the Cybersecurity Summit, President Obama said, "There's only one way to defend America from cyberthreats, and that's government and industry working together [and] sharing appropriate information." However, cybersecurity is not that elementary; there is no one unique way. Furthermore, the associated Executive Order calls for "fostering the development and adoption of automated mechanisms for the sharing of information." That being

so, not only is information-sharing not the “only one way” to improve cybersecurity, but the model proposed for information-sharing is also not the “only one way” to share information.

To explain why requires stepping back to take a broader look at information-sharing. Among the many types of information-sharing, three merit note.

First is the process by which software vulnerabilities are brought to the attention of those who make and maintain software. A large percentage of all networks—particularly the more diligently defended ones—are penetrated because their software contains vulnerabilities that have not been fixed, notably because the vendors have not discovered them. These are “zero-day vulnerabilities”; they permit “zero-day exploits.” Software vulnerabilities in Java, Acrobat, Flash, and Microsoft Office products are commonly exploited to allow attackers to enter computer networks and systems (which is why users are warned not to click on suspect websites or open suspicious attachments). A large and growing community of researchers and white-hat hackers are busy finding these vulnerabilities and reporting them to vendors. A related community examines actual cyberattacks to determine which vulnerabilities were exploited in order to serve the same end of fixing them. A world with fewer software vulnerabilities would be a safer world (although patches do no good until installed). Occasionally, software vendors confronted with a number of similar vulnerability reports about their products may find correlated architectural weaknesses in their offerings and make more fundamental changes. The federal government can do more to encourage and accelerate the process of finding software vulnerabilities with modest amounts of funding and without passing new legislation.

Second is the use of information-sharing to improve cybersecurity *practice*. The collection and analysis of cyberattacks, both those that succeed and those that may be termed near misses, can shed light on what organizations could have done differently to have prevented or at least mitigated the effects of such attacks. Such analysis can provide evidence-based assessments of the cost-effectiveness of alternative cybersecurity tools and techniques. Such an activity is already informally carried out to some extent at the worker level, especially among the information security community and disseminated through professional interaction. This should continue to be encouraged, and should trickle up to the C-Suite and managers. Such activity can lead to insights that are scientifically validated (or refuted), which then become part of the cybersecurity canon, to be spread through the literature and other formal and informal exchanges within the information technology community, as well as taught in the various schoolhouses. The government can aid this process by empowering organizations such as the National Institute of Standards and Technology (NIST) and funding the various Advanced Research Project Agencies (ARPAs) and the National Science Foundation (NSF) to build a systematic body of knowledge.

These first two types of information-sharing do not exacerbate the cybersecurity divide. The first should result in better software, which benefits everyone. The second should result in better cybersecurity practices, which also should benefit everyone, particularly those organizations that have at least one person who can think systematically about cybersecurity.

This now leaves the third type of information-sharing, one that is specific to the characterization of threats and the impetus behind the legislation. It calls for organizations to report attacks and provide relevant details of these attacks, such as malware samples, attacker *modus operandi*, IP addresses, attack vectors, induced anomalies, social engineering methods, etc. These instances, in turn, are used to create a profile of specific threat actors and infer signatures of their activities, which, in turn, would be circulated to other organizations so that they can better prepare themselves, notably by putting such signatures into their intrusion prevention/detection systems. The appendix of the 2013 Mandiant report (*APT1: Exposing One of China's Cyber Espionage Units*), for instance, was stuffed with many signatures that could be used by potential victims of APT1 (their name for a specific hacker group supported by China's Peoples Liberation Army) to recognize signs of threat activity infection. Although such signatures could, and in many cases, would also be supplemented by intelligence collection, the classified nature of such additional material limits the number and type of machines on which they could reside.

The usefulness of threat-based information-sharing rests on four assumptions about the nature of the threat itself. Such assumptions would have to be largely or totally true before the value of establishing an information-sharing apparatus can justify the effort to operate it, persuade organizations to contribute to it, and offset the residual risks to privacy that such information transfer may entail.

The first assumption is that a sufficient share of all serious attacks comes from specific black-hat hacker groups and that each carry out enough attacks over a period of time so that their *modus operandi* can be characterized. Trivially, if every black-hat hacker organization carried out just one attack, signatures derived from that one attack would inform no further attacks. In practice, each group must carry out enough attacks so those that are discovered can inform those that take place later on. Furthermore, for such signatures to be useful, there has to be time for the attack to be detected so that the signatures can be collected, shared, and inserted into the defensive systems of potential future victims while they are still useful. If all the attacks were bunched together in a short period, the information gathered from such attacks will not be gathered in time to be useful.

The second assumption is that each attacker group generates a consistent set of signatures that recur in multiple attacks (and that can be used reliably by defenders to distinguish their attacks from benign activity). To wit, hacker signatures have to resemble fingerprints. The APT1 group's attacks did have such characteristics (similarly, those that attacked Sony Pictures Entertainment in late 2014 used the same IP addresses as those who attacked South Korean banks and media firms in 2013). However, the possibilities of polymorphic malware (variations in the appearance of exploits) and fast-flux DNS (to permit shifting IP addresses) suggest that hackers have options for varying their signatures.

The third assumption is that these signatures are detectable by organizations interested in sharing. The average attacks by sophisticated and advanced threats remain undetected for a year—and those are only the ones that have been discovered. Most such attacks are discovered not by their victims but by third parties and, for the most part, only because the information taken from several victims is funneled through the same intermediate servers used to hold the exfiltrated data. If these servers are discovered, evidence from attacks on multiple victims can be picked up at the same time. Attackers who are sensitive to being caught can explore alternative ways to route the data they bring home.

The fourth assumption is that such signatures will not evolve (enough) over time—even if information-sharing became so widespread that the failure to evolve would make it too hard for hacker groups to penetrate and compromise networks. Although Mandiant's publication of APT1 activities slowed the group's activities, it only took a few months before they were back in business using a new set of exploits and attack vectors, with brand new signatures that had to be inferred.

An analogy may be drawn to the anti-virus industry. The major players—Symantec, McAfee, Kaspersky, and Microsoft—run very large information-gathering networks fed by inputs from customers as well as sensors that they have placed throughout the Internet. But the anti-virus model has lost most of its viability over the past five years in the face of ever-shifting signatures and the practice of attackers testing malware against anti-virus suites before releasing them into the wild. Although threat-centric information-sharing deals with a broader range of indicators than anti-virus companies do, the same dynamic by which expensively constructed measures beget relatively low-cost countermeasures argues against being terribly optimistic about the benefits from pushing a threat-centric information-sharing model.

This is not to say that threat-centric information-sharing is useless. Not every black-hat hacker group will be conscientious about altering its modus operandi, and there may be features of their

signatures that are not obvious to themselves (and hence would likely persist for later detection). Forcing such groups to cluster their attacks or to use multiple attack vectors, including obfuscation techniques and grouping methods, resulting in new or altered signatures over time, means more work for them. Some attackers will drop out; others may not be able to attack as many organizations in a given period. So, the effort to gather signatures would not be completely wasted. Furthermore, even if threat-centric information-sharing does not work, the efforts that organizations would have to make to understand what is going on in their networks in order to share information effectively would, as a side-benefit, also help them protect themselves absent any information-sharing whatsoever.

Unfortunately, these recent efforts to promote a particular kind of information-sharing have achieved the status of a panacea. They are absorbing a disproportional share of the legislative and elite media energy on the topic of cybersecurity. Many otherwise serious people assert that information-sharing could have prevented many headline assaults on important networks. Yet, if one works through such attacks to understand if there were precedents that could have given us threat signatures, one often finds no good basis for such a belief. Quelling the nation's cybersecurity problems is a complex, multi-faceted endeavor not subject to a silver bullet.

In sum, there is nothing wrong with information-sharing. It should be encouraged. The President's proposal may well do so—in which case it deserves our support. But there is something wrong with assuming that it solves most, much less all, of the cybersecurity problem. It only addresses one facet of a very complex space. It is therefore highly questionable whether efforts to achieve information-sharing deserve the political energy that they are currently taking up.

I appreciate the opportunity to discuss this important topic, and I look forward to your questions.