AFCEA International Cyber Committee

CYBER INTELLIGENCE SHARING

Chairpersons: *Richard C. Schaeffer, Jr., Riverbank Associates, LLC; Wray Varley, CenturyLink Government*

Members: *Matthew Coose, Qmulos LLC; Charles Dickens, iCIO, Inc.; Gil Duvall, National Defense University iCollege; Jeff Moulton, Georgia Tech Research Institute; Ricky Windsor, Cyber Cloud technologies*

2014

EXECUTIVE SUMMARY

The original intent of our paper was to explore an alternative. What if we define that "*sharing*" does not involve a detailed set of data that relates to the intrusion (as argued by the opponents of current legislation). Rather, we'd define a set of technical parameters that can be machine-readable, that can be transmitted in real-time, and include ONLY information relevant to the attack structure—the fact-of data that can be used by others to develop or execute countermeasures to the attack. Ultimately, while information sharing is the key requirement, and certainly a much discussed topic, it is Situational Awareness that information sharing facilitates.

Every day, organized criminals and more nefarious actors bombard public and private networks with a massive array of sophisticated cyber attacks. From Distributed Denial of Service (DDoS) attacks and Advanced Persistent Threats (APTs) to other assorted malware that leverages phishing and other delivery mechanisms; they put government and corporate information, assets, and operations at risk. They cause grave damage, and steal the very lifeblood (intellectual property, customer data) of the entities they attack, including the trust in one's brand that may have taken years to establish. These attackers may be well funded or operate as lone wolves. In either case, they are unrestricted by law or custom.

Everywhere one looks there is a plethora of recommendations that fall into the categories of Technology, People and Processes, and Policy. Implementing security technologies and techniques that provide defense-in-depth; educating the workforce and instilling accountability; and tightening policies that support a comprehensive risk management regime are all essential—but it's still not enough. The adversaries continue to get through!

System owners attempt to fight back using the vast array of tools available. In most cases, the defenses are ineffective, reactive, and costly. Real-time knowledge of the threat and collaboration on solutions is many times ad hoc at best. Sharing of information by industry, while growing, is still quite minimal—driven by fear and concerns over privacy and / or lost market share.

The Subcommittee found a great deal of confusion on what is being done and what can be done to address timely sharing of information between and among entities in the public and private communities –

- Information Sharing and Analysis Centers (ISACs) within the Critical Infrastructure, as defined by Presidential Decision Directive (PDD) 63, get mixed reviews on the success of sharing initiatives initiated within the private sector domains they represent. Even when an ISAC does an efficient job of sharing critical threat data, it remains within the boundaries of that particular ISAC. While there are a number of ISACs having success sharing information amongst their respective members, there is little collaboration across ISACs.

- Within the Department of Defense (DoD), the Defense Industrial Base (DIB) Initiative achieved a modicum of success in pushing classified threat information out to a limited set of participants, but the information, while informative to a degree, was neither real time nor actionable in a time frame so as to be effective. In 2012, the Department of Homeland Security (DHS) took over the DIB "pilot" creating the Enhanced Cybersecurity Services (ECS) program, expanding the number of participants from the original base of DoD contractors doing work for the DoD, to all Critical Infrastructure companies (https://www.dhs.gov/enhanced-cybersecurity-services). While the ECS program has the right intent of sharing government threat information with industry, participation is voluntary which could explain why it has been slow to take hold—only two companies are currently authorized to provide ECS service and a very small number of companies signed up to participate.

- Another DHS initiative, the National Cybersecurity and Communications Integration Center (NCCIC), serves as a central location where government and private sector can coordinate and synchronize their efforts. Working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities.

Coordination between and among these entities certainly helps to inform the participating private sector and government community. However, they have little control over the actions taken by the participants. Again, the sharing community is also hindered by the issue of privacy and perceived economic risk of identifying breaches of trust with their clients and customers.

The one bright spot is the April 10, 2014 U.S. Department of Justice (DOJ) and U.S. Federal Trade Commission (FTC) Antitrust Policy Statement[1] on Sharing of Cybersecurity Information that clarifies "properly designed cyber threat information sharing is not likely to raise antitrust concerns." (http://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity).

BACKGROUND

For the past couple of years, the Cyber Intelligence Sharing and Protection Act (CISPA), a proposed law in the United States (U.S.) that would allow for the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies has been the focus of the U.S. Congress and U.S. industries that would be impacted by the law. CISPA's stated aim is to help the U.S. government investigate cyber threats and assure the security of networks against cyber attacks.

The legislation was introduced on November 30, 2011 by U.S. Representative Michael Rogers (R-MI) and 111 co-sponsors. It was passed in the House of Representatives (H.R. 3523, 112th Congress) on April 26, 2012. However, CISPA did not pass the U.S. Senate over threats of a Presidential veto expressing concerns relating to civil liberties, as well as confidentiality issues. In 2013, CISPA was reintroduced to the House of Representatives with numerous amendments addressing several of the issues regarding privacy and confidentiality. On April 18, 2013, the amended Act passed the House of Representatives as H.R. 624, 113th Congress. The Senate is still not planning to review this Act and the threat of veto by the President still lingers over this critically needed interaction between industry and government.

CISPA, an amendment to the National Security Act of 1947, along with several other legislation attempts, is seeking to address the changes brought on by an increasingly hostile cyber environment. While garnering some support from industry, each legislative effort has linked personal and corporate information to the cyber threat or vulnerability reports. The link to personal and corporate information creates the perception of a loss of the expectation of privacy for an individual, and raises potential economic risk for the industry partners.

The climate surrounding the current legislation is not likely to change; while individuals, organizations, and commercial entities continue to debate what should and should not be shared, a spectrum of adversaries continue to take advantage of vulnerabilities in current and emerging technology, poor security practices and the lack of consensus around what to do about it. Cyber attacks from advanced actors continue to grow in frequency and severity, leaving system owners ever more vulnerable because defensive strategies based on present models are just too slow to react to the changing environment. Even with 100% participation and success, CISPA would still result in a wide gap between what is known about adversarial behavior and what can be done about it.

In the current, post-Snowden political climate, it is highly unlikely that CISPA, or any other cyber legislation, will move forward any time soon, further handicapping efforts to create any sort of data-sharing among industry and government.

[1] http://www.justice.gov/atr/public/guidelines/305027.pdf.

DISCUSSION

Notwithstanding the general situation, some government and industry entities are not allowing the lack of action by the U.S. government to inhibit their ability to pursue sharing regimes that meet operational needs while addressing the shortcomings perceived within the CISPA framework. They realize that shifting the balance of power, eliminating malicious actors' advantage, by enabling enterprise owners / operators with a comprehensive well-executed defense is critical. They realize that "active" cyber defense, based on real-time threat awareness and machine-to-machine[2] sharing and mitigation, is the only strategy that will enable confidence in the environment in which government and business operations are conducted.

"Pilot" initiatives have and are being pursued based on real-time sharing of threat information; building the foundation for and proving the efficacy of machine-to-machine real-time sharing of threat information. Conducted in private sector to private sector venues, *e.g.,* led by and within members of the FS-ISAC; public-private venues, *e.g.,* led by and within membership of the National Security Telecommunications Advisory Committee (NSTAC) and DHS; and, a similar entity led by and within membership of a joint DoD, DHS, and the Director of National Intelligence (DNI). These activities have demonstrated advantages that can and should continue to be pursued by a larger nexus of government / industry partners. Some of the advantages and emerging observations include:

- Real-time sharing that can enable the widespread knowledge of the threat environment;
- Improved insight into cyber attack behavior;
- Reduced time to mitigation of many threats as they appear;
- Cross-sector threat views providing a more robust and comprehensive understanding of threats that enable all sectors to more effectively defend their environment;
- Anonymized threat information that can be shared in real time without jeopardizing the privacy of individuals or companies;
- Standards and protocols for "shared threat information," as well as a standard taxonomy of threat terms essential to the success of these efforts; and
- Improved communities of practice and interest supporting mitigation.

In addition to real-time sharing of threat information, these pilot activities have also demonstrated the ability of organizations to share and distribute best practices, share risk management regimes, and promote the establishment of comprehensive Consequence Management analyses that underpin the risk reduction return on investment decisions that every company (and government department and agency) must make as they address increasing cyber threats. To fully realize the benefits of detailed in the pilots, the community must address a number of technical issues related to the definition and adoption of the standards and protocols referenced above. While not universally adopted, two specifications are gaining traction and could emerge as the critical enablers of the desired machine to machine communication of threat information:

- Trusted Automated Exchange of Indicator Information (TAXII™)
- Structured Threat Information Expression (STIX™)

TAXII™ defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries.TAXII, through its member specifications, defines concepts, protocols, and message exchanges to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not a specific information-sharing initiative or application and does not attempt to define trust agreements, governance, nor other non-technical aspects of cyber threat information-sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, enabling organizations to share the information they choose with the partners they choose.

TAXII is the preferred method of exchanging information represented using the STIX™ language, enabling organizations to share structured cyber threat information in a secure and automated manner.

STIX™ is a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information. The

[2] Kenneth Chang, "Automating Cybersecurity," *The New York Times* (June 2, 2014) http://www.nytimes.com/2014/06/03/science/automating-cybersecurity.html.

STIX Language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. Many of the dominant players in the product and services arena are contributing to the STIX conversation and are strong advocates of the TAXII approach to real-time sharing of threat information.

TAXII and STIX are valuable efforts; however, it will be important for them to ultimately be inserted into international standards efforts such that multi-national companies will be able to utilize a globally accepted approach to the automated exchange of threat indicators.

While progress is being made on the technical front, legal issues also still abound. Many companies are concerned about limiting their liability if they share information with each other or with the government, in efforts to inform each other about potential cybersecurity threats. This is a particular point of contention within CISPA itself. As written, the bill grants immunity from lawsuits to companies that pass incorrect "cyber threat" information to the government, as long as the company can prove that it acted in "good faith." This provision was actually the basis for a veto threat from President Obama because the Administration supports "targeted liability protections." The President is concerned about the "broad scope" of liability limitations in CISPA.

Finally, while it is heresy to call capitalism an "obstacle," it is one other issue to be addressed when it comes to companies sharing known threat information. Collecting threat signatures or other threat indicators, and then selling that information to other security providers is a revenue source for many companies. It also helps differentiate those companies in the marketplace. Under what circumstances should companies be "required" to freely share their potentially unique and profitable intellectual property with the rest of industry and the government? What if a business model can be developed wherein the specific information that a company uncovers is actually free for other organizations to use, but the mechanism for obtaining the information can provide a revenue source?

CONCLUSIONS

The Info Sharing Subcommittee entered into this task with a belief that through interviews with various agencies, corporations and individuals, it could produce a White Paper with specific suggestions on how government and industry could share machine-readable data that would include only information relative to a cyber attack in real-time.

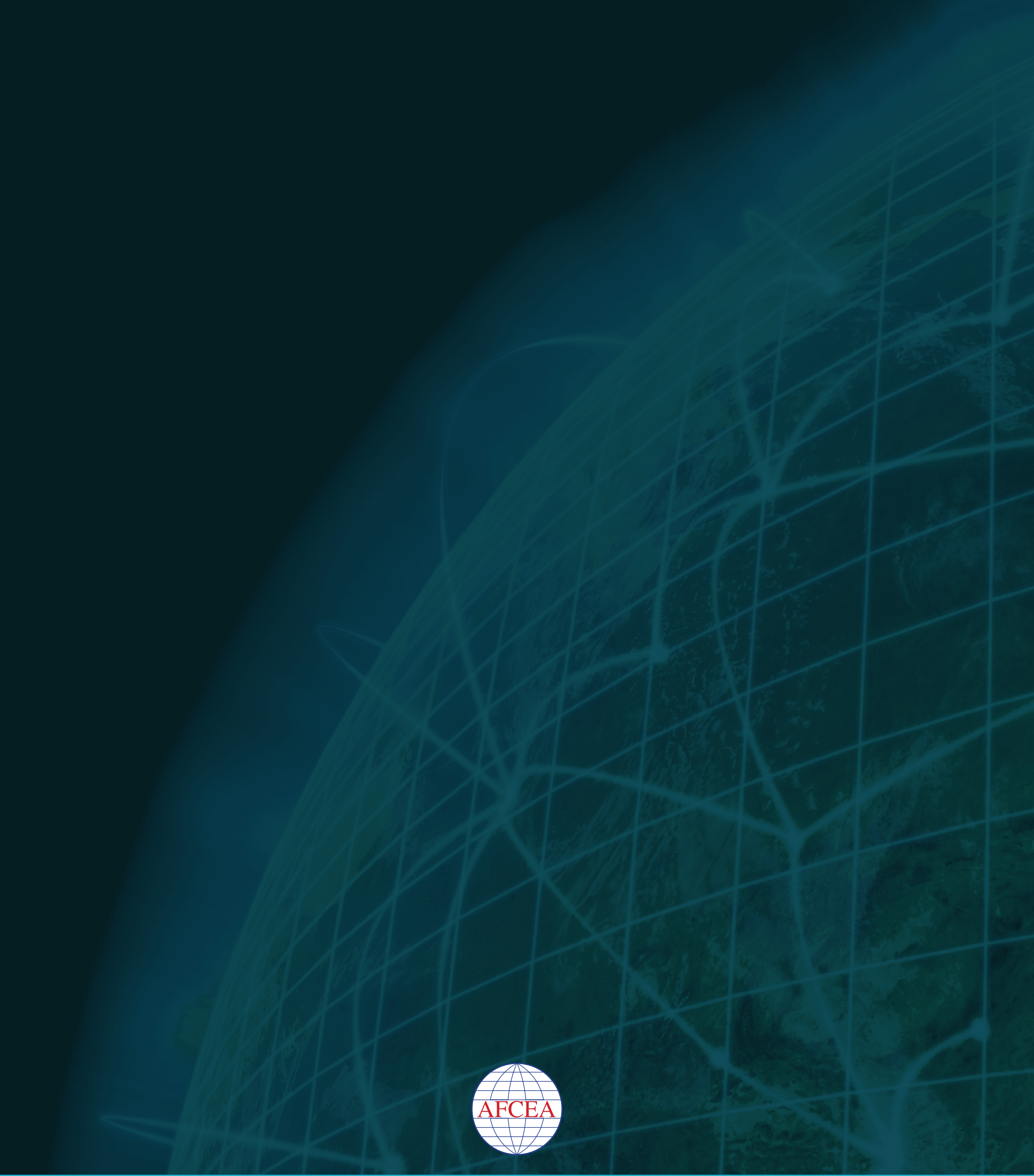
Through the course of our research and discussions, it became evident that -

- it is universally accepted that there is a great need for information and data sharing to help mitigate cybersecurity attacks; and
- technology is not an obstacle; in fact, the capability is currently available.

It also became quite evident that until legislative, legal and, cultural issues are addressed, there will not be an overarching, "standardized" methodology for data sharing among organizations.

The good news is that there are growing pockets of groups who are working within their own ecosystems to share information amongst themselves. Two good examples of these grass roots sharing efforts, but certainly not the only ones, are the Financial Services ISAC and the Tier 1 Internet Service Providers. Both of these groups have devised methodologies to share critical and timely information among their constituents, even when those constituents may be in competition with each other as part of their daily business. Conversely, and ironically, a government entity that we interviewed would not provide our Subcommittee with the permission to include any of their information sharing efforts in our report.

Federal legislation, not agency action or executive branch determinations, is the surest way to make the necessary changes to the legal landscape that is the largest obstacle to overcome. While it has become cliché to say, it may take a "cyber 9/11" to prompt all required parties to take the actions required to implement an information sharing initiative similar to what this White Paper suggests.



The AFCEA International Cyber Committee White Paper Series

www.afcea.org/committees/cyber