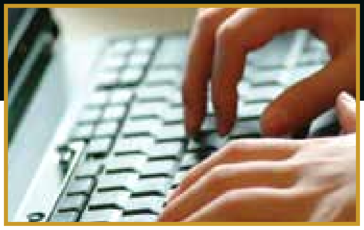
AFCEA

AFCEA International Cyber Committee

PUBLIC/PRIVATE INFORMATION SHARING

By Richard C. Schaeffer, Riverbank Associates,
and James F.X. Payne, Dun & Bradstreet

October 2016



EXECUTIVE SUMMARY

Today's adversaries continue to find new and innovative ways to advance their position against the broad range of lucrative targets, including government, critical infrastructure and the private sector, especially those companies with a global presence. While the number and size of data sources have increased dramatically and information is shared more freely between appropriate partners, critical gaps remain between what's available and what's being used to address one of the most complex challenges to face our nation and its allies. A key finding in the investigations leading to this white paper is that the departments and agencies charged with protecting and defending U.S. government systems constantly are looking for the latest product or service solutions that map the most relevant and current data with the timeliness of the event. Although this could be a technology breakthrough, it is just as or more likely that a process improvement suggestion would have as much impact as the latest Silicon Valley product or service. There is a high level of frustration that the enemy is moving at unprecedented speeds, and it is unlikely that public policy can change fast enough to adapt and morph at the necessary speed to mitigate the impact of our attackers.

This white paper captures some areas of great interest to the cyber community as represented by our sample of interviewees. There is no shortage of practical and achievable process improvement ideas. The overarching theme is that, with the correct and timely level of cooperation between the public and private sector, we can improve our response to cyber attacks and begin to better understand how the *adversaries are attempting to position themselves* in the ever-changing world of cyberspace. There is a need to move from reacting to the traditional attacks we face daily into an environment where, by leveraging the best data available, we can start anticipating—and even predicting—the location of the threat. Our enemies do not attack our infrastructure in random fashion. How can we use all forms of available data to explore the unknown threats and actors? How can we build the trust between and among the government and our various private sector data owners to build these needed models of cooperation?

INTRODUCTION

The AFCEA Cyber Committee is a highly curated team of cyber experts that meet monthly to discuss and promote essential cyber issues. Membership is a balanced group of private sector representatives, government officials and academia. Membership for industry participants requires a nomination by one's peers, submittal of an AFCEA Cyber Committee formal application and ultimately a vote across the entire committee for membership acceptance. Each annual Cyber Committee cycle begins with an extended list of critical issues as nominated by the full team from which a core set of issues is voted upon. The full committee, via a voting/prioritization process, narrows the list and chooses four to six core issues that subcommittee teams are formed to address. These subcommittee teams conduct unique research and initiate cross-industry interviews that result in a formal white paper that goes through peer review and then is published by AFCEA and maintained on the Cyber Committee website.

Jim Payne and Dick Schaeffer co-chaired the cyber subcommittee that created the content of this white paper.

METHODOLOGY

The subcommittee for this white paper identified experts and leaders from various agencies and service providers in the defense and national Intelligence Community (IC) for interviews; interviewees follows. The objective of the interviews was to foster a discussion with government cyber experts that the co-authors hoped could lead to a better understanding of the need for collaboration between government and the private sector, including the types of data that may augment current views. The interviews were conducted with the objective to identify key strategies for leveraging publicly available business intelligence data in alignment with relevant security analytics to enhance the overall effectiveness of cybersecurity programs across the U.S. government. The persons interviewed were selected from recommended sources from the AFCEA Cyber Committee as well as noted experts from the field. The objective of this white paper was not to document problems once again but to seek positive alternatives that could allow both the private sector and the U.S. government to advance their missions quickly and efficiently.

SCOPING

This white paper captures a dialogue between the public and private sectors, allowing all participants to engage in an honest discussion about how to move through what some would say is an impasse. That impasse is the lack of full collaboration between entities that should be partners exploring the dynamic nature of the enemy and their persistent attacks on U.S. corporate and government infrastructures. The segments of this seemingly symbiotic relationship are painfully aware of their respective legal and programmatic limitations.

The paper also examines how to leverage commercially available business intelligence data more effectively to inform and shape security analytics for enhancing the overall effectiveness of the government and, in particular, IC cybersecurity programs. It highlights some of the limitations but more importantly explores current possibilities.

The common starting ground for discussions, the "elephant in the room" issue, is that the interval for response and responsible action can no longer be defined in months, weeks or even days. The threat vector now requires action at cyber speed to minimize the effects of the attack. This requires a much more informed and ready response force with great visibility into the strategies that can make attack prediction a reality.

INTERVIEWS

The following people participated in the interviews conducted for this white paper. None of the comments from the participants were for attribution to encourage as open a dialogue as possible.

Sam Arwood, senior vice president, cyber programs, Sotera Defense Solutions
Thomas Conway, director, federal business development, FireEye/Mandiant
Jim Craft, deputy director for information enterprise management/chief information officer, Joint Improvised-Threat Defeat Organization (JIDO)
Dr. Balakrishnan Dasarathy, program chair, Information Assurance Specialization, UMUC Graduate School
Tim Kosiba, NSA/CSS Commercial Solutions Center (NCSC)
Paul Kurtz, CEO, TruSTAR
John Riggi, former section chief, FBI Cyber Outreach
Dr. Anthony Scriffignano, chief data scientist, Dun & Bradstreet
Steve Shirley, executive director, Defense Cyber Crime Center (DC3)
Gerald "Chip" Willard, senior technical leader, NSA/CSS Threat Operations Center, NSA

PROBLEM STATEMENT

The persistent and constant attack on America's business and national interests is the new reality. The Western world faces a series of enemies who have the expressed purpose of impacting the financial viability of the United States and its allies. The U.S. government has a vital role in protecting the nation from these attacks, as it is charged to assist in the protection of the basic infrastructure on which many U.S. business and government services rely, such as banking, energy, water and telecommunications. For this reason, an essential partnership underlies this mission. All parties have a common goal not merely to survive these threats but continuously evolve their respective campaigns to identify, detect, respond and ultimately deter these attacks.

While the private sector and government are continuously seeking better partnership models, a lack of mutual trust—an essential ingredient—seems to inhibit needed progress. This paper explores areas of collaboration where the government and private sector are collaborating effectively as well as new areas for collaboration that constitute ripe opportunities. For example, the government has access to huge volumes of commercial business intelligence data; however, IC analysts and officers often lack in-depth business backgrounds. Therefore, they may not be able to successfully detect the links/patterns between commercially available business metrics and their own classified data. This white paper explores areas where the private sector and the government can work more collaboratively to integrate commercially available business data and applicable security analytics in a more effective manner to make cybersecurity programs more responsive and timely.

THE ROLE OF INFORMATION SHARING: HOW CAN WE IMPROVE THE MODEL?

Procurement

One might expect procurement issues to be the principal complaint of the business community, rather than government employees. Our interview panel was fairly balanced between the two groups, and somewhat surprisingly, frustrations about procurement came up frequently in our government discussions. A central theme and source of their frustration was that procurement reform often is called for yet never quite delivered. For instance, cyber attack technologies and methodologies as well as public source information evolve rapidly with unpredictable changes happening every day. New ideas and areas emerge in this space as new sources of public information arise such as social media or e-commerce data. This highly dynamic construct however must be addressed within a set of man-made government procurement rules that change at a glacial pace. The U.S. procurement limitations have become a cyber threat. The feeling is that procurement complexity is a key limitation and probably worsening. Procurement should be one of the easiest problems to resolve; yet here we are.

Mission and a sense of urgency should drive the demand for procurement simplicity and reform. This theme was evident in our discussions with the interviewees. Public sector vendors and government leadership seem to share a real antipathy for the procurement process as it exists today. Our U.S. procurement processes are not serving the needs of the mission and lead to a sense of dread and cynicism from both government and industry.

Role of the Traditional ISAC

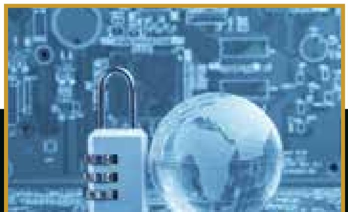
The first formal process the government proposed to assist in cyber information sharing was in 1998. This model was outlined in Presidential Decision Directive-63 (PDD-63). The Industry Sharing and Analysis Center (ISAC) model emerged as a means for vulnerable industry sectors to organize around a process where like-companies could network in times of attack or specific cyber incidents. A number of ISAC models have surfaced in the past 10 to 15 years, but most are challenged by the same inherent problems. Competitors often are reluctant to share sensitive information related to a cyber attack because it reveals the company's vulnerability. In addition, because the nature of the ISAC includes sharing information with the government, challenges have arisen.

The ISAC model is built on trust—trust between natural competitors and trust between the private sector ISAC companies and the government. Is there sufficient trust between the corporate members of the ISAC sector and do these same companies have sufficient trust to be open and forthright with the government? Experience has shown that ISAC organizations attempt to withhold information or obscure the identity of the company. At the very moment when timeliness is essential, a pause occurs. It is at these moments that the limited nature of the ISAC model is revealed.

Cyber Information Sharing Act (CISA)

On December 18, 2015, President Obama signed the annual budget bill for the U.S. government. Within the 14th rider of the 2,000-page document is the Cybersecurity Information Sharing Act (CISA). This legislation has its roots in legislative activities that go back to 2014. CISA, though controversial, does provide legal protection to companies that would share critical cyber attack data with the government. For this reason, CISA is useful and demonstrates progress in the information sharing debate.

The issues that trouble many is that the nature of CISA is voluntary and there is a real concern in the community that the government is not adequately prepared to protect the personal identifiable information (PII) that will be shared with the Department of Homeland Security and subsequently dispersed across seven government agencies, including the NSA, as well as with local police. CISA has divided the industry and heightened the issue of trust between key companies and the information collection process. Though useful in its intent, will CISA foster the free and timely exchange of data during critical cyber events going forward?



MOVE FROM REACTIVE MODEL TO MORE PROACTIVE/PREDICTIVE MODEL

Mergers/Acquisitions

An example that has emerged for future collaboration is the exploration of the possibility of predicting cyber attacks. Cyber attacks are clearly not random. And if not random, what are the characteristics that precede or can be useful in predicting an attack? Can we move toward better anticipation or prediction of cyber attacks? One theory gaining momentum is that cyber attacks may have some relationship with mergers and acquisitions (M&A). Is the enemy using cyber attacks as a means of suppressing stock value of companies prior to an acquisition and/or does the M&A process itself make a company more vulnerable to cyber attack?

On November 21, 2015, *The Wall Street Journal* reported that hackers stole customer credit card and debit card information from Starwood Hotels & Resorts during a breach that lasted for eight months and affected 54 locations, including a number of luxury properties. This breach was reported as the latest in a wave of hacking attacks targeting the hotel industry. In the same article, a reference was made citing that this cyber attack disclosure came only days after Starwood announced it was being acquired by Marriott International, a transaction that would result in the largest hotel chain in the world.

Was the attack related to the acquisition? The M&A process typically makes transparent a lot of data with many potential buyers granted access. Was the attack related to the issue of hotel consolidation? Hotels are not merely a place for vacations or business travel. The site provided Wi-Fi, making hotels the nexus for huge intelligence transfers, including proprietary briefings and passage of critical IP and corporate intelligence.

The Anbang Corporation in China countered the Marriott offer for Starwood, and on March 28 Marriott was reported to have countered the Anbang counter offer. These transactions drove the original Marriott offer price for Starwood up from $12.2 billion to a $14 billion all-cash offer by the

Chinese. Eventually Anbang withdrew its offer and Marriott and Starwood settled on a $13.6 billion deal in September.

The above scenario is a perfect example of how the government can leverage publicly available data to explore these possible interdependencies and use the results of the collaborative research to get closer to a cyber model that can predict future cyber attacks. Both vectors bear exploring, the M&A model as well as the possible consolidation of the hotel industry model. These two examples are rich with public data that when mapped against the classified information within the Committee on Foreign Investment in the United States (CFIUS), for example, could expose the interdependency of what until now may appear to be totally independent events.

Third-Party Commercial Model for Cyber Alert

Alternative private sector third-party models, which that have a “post-to-all” approach where member companies share directly with each other, have emerged. The private sector model allows carefully screened and curated participants to share highly specific attack parameters in real time with member companies. The identity of the member company is protected within this business model where the company that is sharing the information is anonymous to all participants, even the host third-party company. Even with a court order, this identity protection system cannot be breached. Theoretically, the government can be a subscriber to this approach, but like all other members/subscribers, they will only have access to anonymous information.

It should also be pointed out the government can and often does make a compelling argument to convince the targeted company to share critical cyber attack parameters. Many times knowledge of the cyber attack can start with a government. This early alert can come from an agency cyber mission command center and then be shared with the targeted company. The challenge here is that, with limited staffing, this cyber outreach is typically done on a company-by-company basis, has time restraints and cannot scale. What is emerging is a complementary set of choices where the government has its approach to collecting cyber attack information but at the time a commercial solution also is emerging. The anonymous data reduces the level of trust needed to execute an early-alert model.

Discovery of Unknowns

Data scientists in the private sector continue to look creatively at the evolution of business data in the context with myriad of additional uncurated or unknown data that can be discovered, curated and synthesized into a relevant and connected context. This capability relates to the ability to cast a very large set of known entities into a connected set of relationships. By applying a set of rules and conditions, one can project these relationships forward in time to represent various scenarios and then form inferences: discovery of the unknown based on what is known. This approach requires the important collaborations between the IC worlds with their unique data sets. When this intelligence data is melded with the structured or often unstructured data commonly available from public sources, a powerful partnership can emerge.

The government currently lacks simple ways to bring these needed partnerships together because this can mean sharing highly classified information. This creative model requires expedited means to bringing the partners together to evolve the data as well as the underlying algorithms that are needed to illuminate the data.

Transfer of Technology Through the Transfer of Humans

Information sharing also can mean sharing human resources between the private and public sectors. Industry often talks about the "war for talent" and the need to attract and retain the most desirable employees. Conversely, the government laments that its low employee turnover causes agencies to miss out on the talent refresh that is inherent in the daily churn of business. As a result, the long-term agency employee becomes married to an established process and is sometimes not incentivized to explore new innovative methods to address the unknown element of the problem, such as an IP address with no corporate context. Agencies now are becoming worried that their low-turnover "come to the government and retire" strategy perpetuates a less-than-creative culture. Fortunately, some government entities are beginning to challenge this precept and pursue a work force where government service is but a part of an overall career.

During one of our interviews, we actively discussed the concept of technology transfer through the transfer of humans. There is a more dynamic model associated with the new technology often called virtual companies. This is seen as the more adaptive model lacking in the federal government career cycle. There is a need to bring in fresh perspectives and thought processes that will enable the infusion of new ideas and creative thinking.

At some point in the interview it almost felt as if we had switched sides of the table. The government was actively seeking a more disruptive model. The concern is government employees feel too safe and therefore avoid the risks inherent in working for a high-profile cybersecurity technology company. There was an active discussion about how to influence employees to move out of their government positions to the private sector. This technology transfer was considered positive, as it would give the government a means to insert its thoughts into the private sector companies in which their employees migrate. There is a call for government employees that could be detailed temporarily to the private sector or short-term internships should be created.

Recommendations

As with most complex topics involving changing conditions and views, we found strong indicators that the people involved in the day-to-day activities of cyber operations would welcome a fresh set of ideas, whether these perspectives come from the private sector or from employees new to a U.S. government career. This was a welcome observation and provides an opportunity for government agencies and the private sector to continue pursuing mutually beneficial ways of addressing one of the most complex problems to plague our modern culture. So, what should we do?

- Identify exceptions to existing acquisition policies that can be piloted to demonstrate the value proposition in “rapid acquisition” and leveraged to make the response to known cybersecurity issues a normal activity rather than the heroic actions required so often today.
- Identify opportunities for government entities such as the Department of Homeland Security or FBI charged with protecting and defending government systems and networks to work with private sector entities that have access to data sets that fill the gap in government knowledge—the unknown knowns. Create working examples!
- Create pilot programs where the parties can come together, share technology, tactics and possibly personnel, such as data scientists, and then assess the value proposition in leveraging data not usually available to government entities.
- Operationalize what works and foster more widespread adoption across the government.
- Assure that private sector entities understand the value of the data they make available, breaking down classification barriers that may be an inhibitor to complete understanding.

The AFCEA International Cyber Committee White Paper Series

www.afcea.org/committees/cyber