STATEMENT FOR THE RECORD OF
TRISH CAGLIOSTRO
HEAD OF GLOBAL GOVERNMENT SOLUTION ARCHITECTS
ANOMALI
BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
CYBERSECURITY AND INFRASTRUCTURE PROTECTION
SUBCOMMITTEE
ON MAXIMIZING THE VALUE OF CYBER THREAT
INFORMATION SHARING
NOVEMBER 15th 2017 | HOUSE CAPITOL VISITOR CENTER

Chairman Ratcliffe, Ranking Member Richmond and distinguished Members, I am honored to appear before the Committees today to discuss how we can improve the partnership between the public and private sector to improve our nation's security with cyber threat information sharing.

I work for a leader in the Cyber Threat Intelligence space called Anomali. At Anomali, we have worked closely with the public and the private sector to enable information sharing for several years. My role is to lead a team of professionals in the global public sector to solve the biggest challenges in leveraging threat intelligence to stop critical threats and facilitate relationships between industry and the public sector.

Anomali was the first company to automatically share intelligence back to the Department of Homeland Security's Automated Indicator Sharing program, referred to as AIS. We also integrate AIS information with our technology and provide access to approved customers. Our deep integration with AIS and experience with facilitating cyber intelligence sharing communities provides unique insights into the critical factors for successful sharing programs and opportunities for improvement in the AIS program.

In my testimony, I will describe the state of threat intelligence in the private sector, how we can reduce the barrier to entry for the private sector to share information through AIS and improve the quality of information provided by AIS.

State of Threat Intelligence

In 2017, the Ponemon Institute commissioned a report: The Value of Threat Intelligence: A Study of North American and United Kingdom Companies that included over 1000 respondents. (https://www.anomali.com/resources/whitepapers/value-of-threat-intelligence-ponemon-study) This report provides valuable insight into how the private sector uses and consumes threat intelligence. The report found that 80% of organizations use threat intelligence and of those organizations, 84% identified threat intelligence as essential to a strong security posture.

One of the biggest challenges identified by 70% of respondents was the volume of available threat data. Today, there are over 400 million indicators of compromise in the Anomali platform and we have seen the volume of threat data from open source, shared intelligence and threat intelligence vendors grow exponentially since our inception. Threat Intelligence Platforms like Anomali enable organizations to aggregate and consume the overwhelming amount of threat intelligence available to organizations.

The biggest value of threat intelligence is the ability to integrate with an organization's security controls to detect and prevent malicious activity on the network. 65% of respondents cited integration as necessary to maximize the value of threat intelligence data. Think of the No-Fly List that airlines use to prevent threats from flying. If the data wasn't integrated with airline and airport security systems, the value of the list would be diminished because it couldn't

prevent high risk passengers from flying. Threat intelligence integration provides the cyber no-fly list by integrating with security controls to detect and prevent threats.

Once an organization can consume and integrate threat intelligence, they have reached a maturity level where they are ready to share intelligence. 62% of organizations reported that they share intelligence. Of those organizations, 50% share with trusted security vendors and 43% share with trusted peer groups while only 30% of organizations reported sharing with the government through programs like AIS and CISCP. Organizations identified a lack of threat intelligence expertise as the primary reason why they do not share intelligence.

When we think about maximizing the value of information sharing in the context of AIS, we need to keep in mind the state of threat intelligence in the private sector. In my experience, these challenges are also relevant in the public sector. You have to help yourself before you help others and organizations in both the public and private sector need the tools to handle the overwhelming amount of threat data and integrate the intelligence before they are ready to share intelligence. When they are ready to share, trust and ease of use are critical for success.

Barriers to Entry for Private Industry

The barrier to information sharing through AIS and the quality of information provided by AIS are intimately related because a significant portion of the information provided by AIS is shared by the participants. If participants do not share valuable information through AIS, the quality of the information that is delivered will be impacted. The level of effort to share intelligence through AIS and lack of expertise in threat intelligence act as barriers to entry to share intelligence through AIS.

When an organization wants to connect to AIS, they must sign a terms of use document, setup a TAXII client, purchase a PKI certificate from a commercial provider, provide your IP address to DHS and sign an Interconnection Security Agreement. While this may not seem overly complex, this process can take private organizations weeks to complete because of legal reviews and change control processes. In the public sector, this can be even more time consuming because additional processes and requirements can cause delays due to the time to get new technologies online.

Once an organization is connected to AIS, they often find it difficult to share intelligence. While there are a variety of options available to private industry to share with AIS including TAXII client software, a DHS website and email, they add additional work for analysts outside of their workflow. Almost every organization is struggling with the resource shortage in cyber security, and adding additional work to share information will negatively impact participation rates.

There is an extremely limited supply of skilled threat intelligence analysts. When organizations share intelligence, they may be concerned that they do not have the expertise to produce relevant intelligence that other organizations will find useful. Organizations are afraid to be the

boy who cried wolf and look immature for sharing intelligence that other organizations will not find useful.

These challenges are common for any information sharing program and are the first hurdle that Information Sharing Analysis Organizations and Centers or ISACs and ISAOs must overcome. Anomali is the technology platform for several ISACs and ISAOs and has identified several solutions to reduce the barrier to entry for organizations to share that can be applied to AIS.

When a new ISAC or ISAO partners with Anomali, the timeline for their members to gain access and start contributing is extremely short. ISACs and ISAOs are provided with their own instance of the solution and the members are automatically added to the platform. They simply login to begin collaborating rather than waiting to deploy technology in their own environment. We also work with the ISACs and ISAOs to provide member outreach and deliver training so companies feel comfortable with the solution. There is data already present in their instance from open source and the ISAC which provides immediate value to the analyst. The AIS program would benefit from continuing to partner with third party organizations like ISACs and ISAOs an security vendors like Anomali to streamline the process to gain access to AIS.

Analysts collect and produce cyber threat intelligence as part of their daily workflow. In the Anomali platform, analysts simply check a box to automatically share intelligence with their community. They are more likely to share because it's integrated with their daily workflows, rather than an additional step or technology they must work with. The AIS program will benefit from outreach by DHS to the security industry to further integrate sharing with the technologies that analysts use every day.

Analysts on the Anomali platform have a variety of options to contribute that range from providing net new intelligence to enriching existing intelligence. Analysts benefit from the diversity in sharing mechanisms because they can participate at the level they feel comfortable. Not all organizations produce net new intelligence and allowing analysts to enrich existing intelligence with data like sightings on their network or associations to an actor makes sharing less intimidating and reduces the level of experience an analyst needs to participate. The AIS program can benefit by expanding the types of intelligence analysts can share beyond just indicators of compromise.

Quality of Intelligence

Measuring the quality of cyber intelligence can be incredibly difficult because the value will vary based on who the organization is and how they use threat intelligence. At Anomali, we work closely with our customer base to more intimately understand what factors impact the quality of intelligence they are leveraging. Ultimately, when discussing the quality of intelligence, organizations want relevant intelligence. They want to understand out of the millions of indicators that are available, which ones need their attention. Relevant intelligence is extremely powerful because it helps drive response and reduce time wasted on low priority information.

Think of cyber intelligence like a weather report. If I told you it was going to be 65 degrees, would you wear a jacket? Before you made your decision, you would want to know contextual details like where did I get the report from, has my source been accurate in the past and when and where it was going to be that temperature. If I am a trusted source, you may just take my word for it because I know what makes the report relevant to you. If I knew that it is going to be 65 degrees, I would wear t-shirt and shorts. If you are like my college roommate from California, it's time for the down jacket.

Like the weather example, organizations derive relevance from context about intelligence and the organization's own requirements to make decisions. The more context they have about shared intelligence, the easier it becomes to determine if it relevant and select a course of action. In the Anomali platform we enrich threat intelligence with the contextual data and provide the tools that organizations need to easily identify relevant intelligence. Our data model has defined threat intelligence objects supported by flexible fields that allows organizations to capture and store additional types of contextual data.

Today, AIS information has limited context which impacts the private sectors ability to determine relevance and determine the appropriate course of action. Organizations look at factors like the source, confidence level, impact type, timeliness, and sightings among other factors to determine relevance. The next iteration of AIS supports STIX 2.0 which expands the AIS schema to allow for more context which will improve the quality of the AIS data.

Conclusion

When I first started at Anomali, people often asked how we forced people to share intelligence. People assumed that when we talked about sharing, we had to be forcing people because no one would choose share unless they had to. Our approach wasn't to force people to share, but to create an environment where sharing was easy and organizations received value.

The AIS program has come a long way since it's inception and as the barriers to entry are reduced, more organizations will participate and increase the quality of the data provided.