AVIATION ISAC

August 2024

Leaders must change the culture of their organizations to better protect critical infrastructure.

"Without trust, we don't truly collaborate; we merely coordinate or, at best, cooperate." — David Horsager

In the context of cybersecurity and information sharing, this quote reveals that we have miles to go in the journey toward successful collaboration between the government and private sector. The passionate cybersecurity experts in both the government and private sectors have been stuck in cultures which have yet to fully recognize the capabilities and passions of each other. This lack of recognition and trust inhibits the timely sharing of valuable intelligence which will protect critical infrastructure. We must break down the cultural and process barriers to information sharing which are holding us back from true collaboration.

A significant portion of the assets which make up the nation's critical infrastructure are owned and operated by the private sector. Using aviation as an example, whether the next most significant cyber-attack is made upon a government owned airport or a privately owned airline, it could equally lead to an impactful degradation of the aviation infrastructure. We must build a sustainable culture which defaults to the timely exchange of actionable intelligence between the government and the private sector.

If you want to change the culture, you will have to start by changing the organization. – Mary Douglas

Over the past decade, the government has made some great progress in cyber defense of critical infrastructure, so to the private sector. Little of this progress has been made jointly. Both the government and the private sector must change their perspectives and their information sharing cultures. **We must drive a major shift in cultural thinking of those who collect and manage intelligence. The pivot is simple yet monumental. Our government must move from the mindset of "hold onto this intelligence because the collection method is sensitive" to "we must find a way to share this intelligence because it could hurt our infrastructure, economy, and citizens."**

On April 30, 2024, the White House issued the National Security Memorandum on Critical Infrastructure Security and Resilience, stating "While most of the Nation's critical infrastructure is owned and operated by non-Federal entities, which are primarily responsible for individual assets' security and resilience, both Government and the private sector have a mutual responsibility and incentive to reduce the risk to critical infrastructure." This white paper addresses the key obstacles to effective government and owner-operator information sharing which is essential to all parties reducing cyber risk. This paper also provides actionable recommendations to improve the culture and mechanisms of information sharing between the government and private sector.

There are government entities which have dual responsibilities as the provider of a critical infrastructure service and as a regulator. We must build a wall between those functions in order to accelerate the sharing of cyber information between the private sector owners and operators and the government operators.

Key obstacles to government and private sector information sharing

- The culture is stuck in old thinking, such that the government must hold onto sensitive cyber threat intelligence for a law enforcement investigation, or to protect a source or method.
- Owner operators "need to know" is not recognized, nor well understood.
- Information classification assessments do not adequately consider "infrastructure resilience" as a driving factor to do more work to get information to a level shareable with owners and operators of critical infrastructure.
- Some government agencies are both a regulator and a provider of a critical infrastructure service.

Culture: We have seen positive changes in the sharing of cyber intelligence by the government in recent years. The information sharing around the Volt Typhoon campaign is a good example. We need to accelerate this change and continue to knock down the barriers to more timely sharing of actionable intelligence.

The most significant obstacle on the government side of the ledger is the culturally embedded disposition to not share cyber intelligence information because of its value to law enforcement or national security and/or to protect sensitive collection methods. These priorities are important, but they are not properly balanced with the priority of keeping critical infrastructure resilient. The government needs to accelerate a cultural shift from "we can't trust the owners and operators of critical infrastructure with this information" to "we must share sensitive cyber intelligence with the owners and operators as part of the strategy to keep critical infrastructure operational."

Need to know: This challenge of when to protect and when to share intelligence is one the US government struggled with prior to September 11, 2001. Then, the issue was government agency to government agency:

> "But the security concerns need to be weighed against the costs. Current security requirements nurture overclassification and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for information sharing…Agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration."[1]

What was a government agency to agency issue, still exists in the government to private sector arena.

Changing culture is a long, slow process. It requires extraordinary leadership, repeated communication of the vision and behaviors expected of the team. Cultural shifts require policy and process updates, empowerment, and systems of rewards and accountability. Across the globe some governments have made this cultural shift, many are slogging through the process, and

[1] https://www.9-11commission.gov/report/911Report.pdf page 417

others, have yet to embrace the need for this change. This has been validated as one government shared "sensitive" intelligence with the aviation industry and over a year later, the US government shared the same "sensitive" information. Why was one so far ahead of the other in sharing sensitive information? Culture.

There continues to be a gap in the communication of intelligence requirements. The private sector has noted that the names of victims is not needed nor wanted. Attribution to the attack groups, though sometimes helpful, is not a requirement. What is a requirement is timeliness of the sharing of indicators, tools, techniques and processes (TTPs). A bonus would be some context around the collection, however the timely sharing of indicators and TTPs is essential.

Information classification assessments: As the 9/11 reported cited the need to break down the culture of hoarding intelligence, we need to increase sharing between the government and the owners and operators of critical infrastructure. This process begins with initial assessments as to the classification of collected intelligence. With respect to the government's creation, collection and classification of cyber threat intelligence, the reluctance to share often stems from well founded concerns over compromising sources and methods of intelligence collection. The private sector understands these concerns and recognizes the sensitivity of the collection sources and methods, as well as the concern that leaks could jeopardize national security and law enforcement operations.

However, the private sector owners and operators manage assets that are vital to national security, economic stability, and public safety. This creates the "need to know" actionable information that could preempt or mitigate cyber-attacks.

In almost one third of incidents, ransomware was deployed within 48 hours of initial attacker access. Seventy-six percent (76%) of ransomware deployments took place outside of work hours, with the majority occurring in the early morning.[2] The swift capabilities of the attackers also underscores the owner-operators' need-to-know in a timely manner.

Collectively, we need to challenge our assumptions that cyber intelligence collected from sensitive sources could only be tied back to that one sensitive collection source or method. For example, law enforcement may collect indicators of compromise and malware from a ransomware victim. This information is deemed "law enforcement sensitive" and thus not shared with the owners and operators of other critical infrastructure. That is the easy thing to do, just not share it. However, this information is about an **on-going threat** to all the other owners and operators. The hard work is for the government intelligence collectors to find out how to get this information out to the other owner operators in a timely manner.

Expedited sharing of information describing attack methods and other indicators (without disclosing current victims) could prevent or assist in the detection of additional attacks. Government agencies must go beyond the sensitive collection method and ask themselves

[2] https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools

whether the intelligence may reside in multiple places on the internet. If so, is the original source or method of collection really at risk? Is an investigation involving one or more current victims more important than preventing additional companies from victimization? This is a major shift in cultural thinking from "we must protect this intelligence because it is sensitive" to "we must find a way to share it because it is dangerous."

Our priority should not be the investigation involving one company but rather the resilience of the many companies which operate aviation critical infrastructure.

Over and over, we see the attackers are indicted and reside in a country or countries which will not extradite them. Clearly this tilts the priority toward sharing intelligence immediately and not a year or more after an attack has occurred.

This requires a significant cultural shift. From the hero mode, which is that wherein the government sees itself as the hero, arresting the attackers, to a community policing strategy, wherein the governments and private sector work together to reduce the impact these attacks could have on critical infrastructure.

Separating the regulator function from the real time threat intelligence sharing function.

There are government entities which operate structures and or services that make critical infrastructure run. The Federal Aviation Administration is a good example. They are an industry regulator and provide air traffic control services and operate ATC networks and technologies. The government must build a wall which will ensure private sector sharing of threat intelligence with an agency which has such dual functions, such that only the operators of the services have access to the information. This will increase the effectiveness of sharing as it will be only the operators accessing and actioning the data. The regulator portion of the government entities would still have access to mandatory reporting and can use that information to impact policy.

Regulators do not need access to real-time cyber incident response information. The regulators should be focused on policy. Policy should not be drawn up in the heat of the battle, but based on thoughtful review and analysis of after action reports. The incident responders are the only ones who need the immediate exchange of information to maintain operational effectiveness of the critical infrastructure.

Recommendations:

- Expand the vision of cyber intelligence collection agencies to specifically include the enablement owners and operators of critical infrastructure to remain resilient despite continuous cyber-attacks on critical infrastructure assets.
- Modify or enhance policy, organizational structure, processes, metrics, and compensation to drive the sharing of actionable cyber intelligence.

Strategy

Many global government entities have strategies which advocate for government entities to share information with the owners and operators. In some cases, it is working but in many more it is not.

The government should embrace the owner-operators' passion for their businesses and customers. This passion has led to the development of outstanding cybersecurity teams in the sector's leading companies. Through trusted communities like the Information Sharing and Analysis Centers (ISACs), owners and operators (and in some cases government entities as well) are raising the cyber skill levels of the industry. The government should not be competing with these efforts, but rather partnering, and accelerating risk reduction via the private sector communities that have been curating trusted communities and driving intelligence sharing and best practices.

Organizational Structure

The government must separate the operational aspects of departments and agencies from the regulatory functions. The separations must be well defined, preventing those in regulatory positions from having any influence over the intelligence operations of those in the operational functions. This will enhance trust, accelerate information sharing and make the critical infrastructure more resilient.

Processes and metrics

Cultural shifts require government leaders to challenge their departments and agencies and create measures of success to drive new behaviors. All agencies investigating cybercrimes need to measure how quickly actionable intelligence was disseminated. They need to devise ways for the private sector to provide feedback that government-provided cyber intelligence led to either the discovery of a breach or the prevention of one. Celebrating these successes will change the culture.

The government should increase analyst-to-analyst meetings with the owner-operators during cyber-attack campaigns. The focus of these meetings should be on sharing information which would allow both the government and the private sector to build a comprehensive picture of the campaign, leveraging industry tools such as the Mitre ATT&CK framework.

Conclusion

To truly embody the essence of collaboration, both governments and private sector owners and operators of critical infrastructure must refine their strategies, cultures, and organizational designs. By addressing the issues noted in this paper and implementing the recommended strategic improvements, there will be a more robust defense against cyber threats. The journey of working together successfully requires not just coming together but evolving together in a continuous, trusted partnership. This will lead to resilience.