Subject: Response to Information on Current and Future States of Cybersecurity in the Digital Economy

Name: Paul Kurtz and Shimon Modi
Company Name: TruSTAR Technology

Topic: Critical Infrastructure Security

Executive Summary

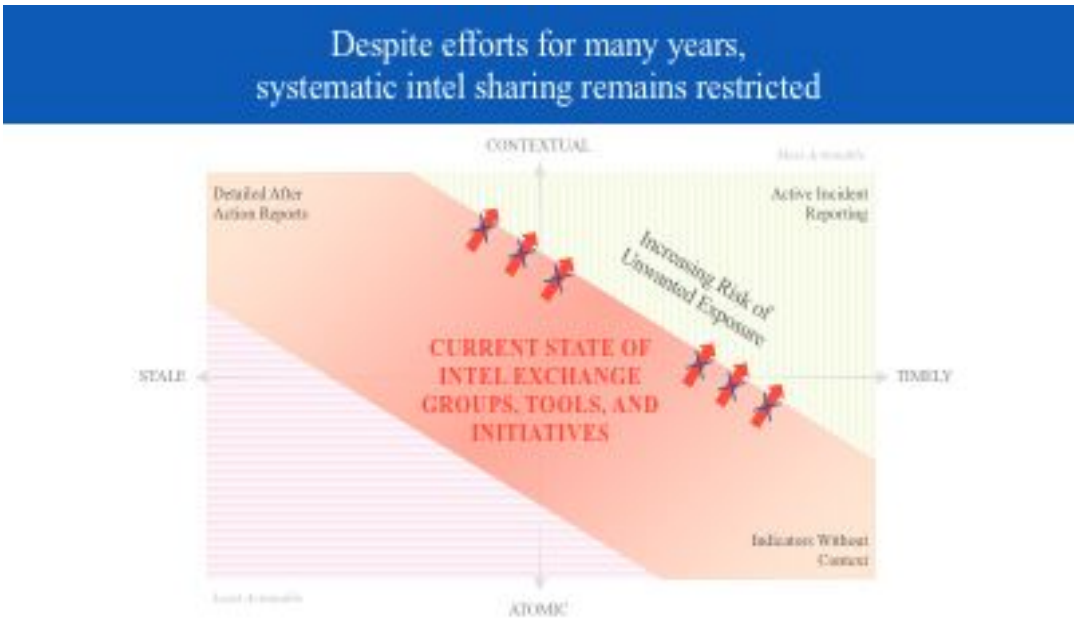
We believe creating effective incident exchanges is vital to security of critical infrastructure. Such exchanges must solve for two problems at the same time: protection from market and reputation risk and provide immediate return to those exchanging incident data. SACs, ISAOs can serve a very important role, particularly in establishing best practices, procedures and common nomenclature. However, we do need to focus on B2B technologies which solve for protecting market and reputational risk and provide return on investment.

The Current State of "Sharing"

As the Commission knows, In the past few years we have seen the number of coordinated attacks increase and organized cybercriminal activity proliferate. Adversaries are taking more strategic approaches, refining their techniques and targeting of victims to improve their infection rates. The changing nature of physical and digital operations is opening up critical infrastructure to increased risks that can have massive consequences for national and economic security of the United States. NIST's Framework for Improving Critical Cybersecurity Infrastructure is a step in the right direction as it offers organizations and operators an approach for evaluating risks and improving security and resilience of their systems. But the threat landscape is changing rapidly and it will be important for operators and owners of critical infrastructure systems to leverage the framework to its full effectiveness.

One recent significant change in the threat landscape is that criminal communities oftentimes share strategies and tools and sometimes combine forces to launch coordinated attacks. They regularly use underground marketplaces to sell plug-and-play malware, exploit kits, and buy and sell stolen information and identities. According to Verizon 2015 Data Breach Incident Report (DBIR), 75% of enterprise attacks spread from the first company to the next within 24 hours. The spate of ransomware attacks on healthcare providers in the first half of 2016 is another data point indicative of repetitive and recycled attack strategies. Even though NIST's framework acknowledges information sharing in *Respond* function of the Framework Core, our viewpoint is that existing information and incident exchange methods and lack of clarity on technological approaches is limiting our ability to improve security and resilience of critical infrastructure systems.

“Sharing” has taken on a negative connotation given companies often believe that if they share in a more structured environment they can expect little in return. When data is exchanged it is often dated and without context and therefore not actionable.



Incident Exchange Challenges

Some cyber incident exchange is being practiced today, but it’s limited to close peers, or personal trust-based business relationships. This form of incident exchange does not scale with the rapid spread of attacks. Trying to operationalize information from such relationships can be challenging as most of the data is shared over emails or other forms that are not readily machine readable. Relying solely on real world relationships to assure secure collaboration also limits the overall reach and impact of these forums. Sector specific efforts are underway too in form of information sharing and analysis centers (ISACs) and ISAO’s to track industry specific cyber attacks and collectively develop defenses. Sector specific ISAC’s stay separate to protect their member’s privacy or believe that attacks in other sectors are not relevant to them. President Obama’s Executive Order 13636 of 2013 provides for the creation of Information Sharing and Analysis Organizations (ISAOs), but much work remains to be done over the next several years to provide the guidelines for the designation and operation of such organizations. The perception of government involvement and close ties to government data collection often reduces active engagement by the private sector because of concerns over additional regulation, oversight and liability.

There is also confusion between the functions of threat intelligence and incident exchange and their implicit value to an organization's security posture. They are both important for improving security posture but they are not the same. The former most often involves the deployment of sensors to detect potentially malicious activity in the wild, while the latter involves sharing active incident information. The information companies receive through threat intelligence platforms could be of vastly different relevance based on how and where it was collected. For example, some tools are driven by honey pots and while interesting they don't necessarily include information about actual attacks which means companies receive false positives and/or data that isn't actionable.

Barriers to Incident Exchange

Reputation and Risk Profile Ramifications: Companies fear the negative impact on their brand, customer trust, and bottom line when an incident is disclosed. Can companies disclose incidents such that they are beneficial to others while at the same time not incurring a negative impact on company brand and reputation?

Adequate Liability and Regulatory Protection: Legal concerns have also hampered the sharing of cyber security information. What if a company shares information without malicious intent but the information is mistaken? That company could be sued for damages resulting from the error. Or a company fears new or additional regulations ranging from increased Federal Government reporting to mandatory security measures.

Perceived Market Disadvantage: Many companies fear that sharing sensitive cyber incident information could have negative business repercussions and render them less competitive. It feels like there is more risk and uncertain reward to share. What value will companies receive for sharing?

Privacy and Ensuring Data Security: This concern surrounds the desire to assure the integrity and confidentiality of both submitted data and system contributors, including the desire of contributors to retain control over their data and how it is used. Can companies share data and be assured it is only be shared with vetted companies?

In addition, companies now what to share data not only within their sector but with other ad hoc groups and individual companies that may be providing support such as consultants and legal counsel.

Addressing Challenges in Near Term (1-2 years)

Our viewpoint is that critical infrastructure needs a connective defense framework, enabled by a systematic platform approach for anonymous incident exchange and collaboration. The goal of the connective defense framework would be to facilitate effective prevention techniques and faster detection times among public and private sector organizations. The Cybersecurity Act of 2015 provides a foundation for such an approach as it mitigates many of the risks outlined

above and enables private companies to exchange cyber incident information. This act gives the public and private sector an opportunity to create a connective defense network, but if we keep sharing information at human speed we will never be able to close the gap with the speed at which attacks are happening.

An effective incident exchange and collaboration platform should encompass the following:

- Trustworthy
- Privacy protection, including redaction of PII
- Anonymity, when needed
- Capable of exchange with multiple secure communities
- Immediate value to operators through correlation and enrichment
- Secure Collaboration
- Automated Indicator Extraction
- Automated Indicator Sharing
- Alerting and notifications

Building a Reference Architecture

There is a growing body of knowledge focused on best practices and standards for cyber information sharing. But there is a gap in frameworks that help operationalize incident exchange and collaboration. NIST and other federal bodies should focus their activity on building repeatable reference architectures for incident exchange that map back to NIST's Cybersecurity Framework. Private and public sector entities are already developing their own toolsets to address incident exchange - a repeatable reference architecture of technical capabilities will keep pushing our ultimate goal of a stronger security posture in a positive direction.

Summary

A significant amount of progress has been made towards building a more secure and resilient critical infrastructure due to the various efforts of public and private sector organizations. In this public comment we have identified challenges posed by the changing threat landscape and a solution framework that addresses these challenges. The framework we are proposing recognizes the progress made in recent years as well as the gaps that need to be filled to realize a more secure critical infrastructure.