Unified Threat Sharing and its Consumption via Machine-to-Machine (M2M) Analytics – A Possible Future Scenario

By: Ken Foster, 5/23/2015

Forward: This discussion covers the concepts of the upcoming STIX, TAXI, and CybOX standards and how those concepts might be woven together to enhance overall cyber security. These standards are still in a state of flux and while there are notable industry early adopters, there is much work to do prior to achieving a fully integrated multi-vendor solution. However, with government regulatory, industry standards adoption, and due diligence pressure applied from the Cyber Risk Insurer industry, the potential for reduced cyber risk across networks, providers, and organizations is significant. This paper will explore one such best-case scenario as a basis for how the model could provide these benefits.

Assumptions applied to the papers scenario:

- This scenario take place in the foreseeable future
- Federal government mandates STIX, TAXI, and CybOX on all current / future contracts driving integration by vendors
- International regulatory standards embrace the CybOX cyber-information sharing model
- Cybersecurity providers commoditize cyber intelligence services and offer Intelligence-Feeds-as-a-Service (IFasS) into STIX and CybOX at economies of scale that both sustain a viable business model and make it affordable to the masses at all business size models
- Legal and private risk providers require enhanced cyber intelligence analysis as part of legal and private Due Diligence standards of conduct
- Legal protections related to information sharing successful are passed in to Federal law and States do not impede said standards with counter-productive additional regulations
- Tighter integration of vertical industries will produce specialized tactics and trend analysis for their partner organizations, enhancing and focusing cyber intelligence products

Scenario: Ubiquitous Enterprise International (UEI) is a medium sized manufacturing business located in Middle America. UEI manufactures internet connected widgets and sensors for the burgeoning Internet of Things (IoC) integrator industry. As such, UEI's network allows several of its foreign manufacturers to integrate with its Just-in-Time manufacturing systems to facilitate component ordering. This has made UEI's Intellectual Property (IP) a target of past industrial espionage attempts. UEI employs firewalls, Intrusion Prevention Systems, subnet and VLan isolations of SCADA manufacturing systems, and endpoint security mechanisms. UEI ties event reporting from all these mechanisms into a Cybersecurity dashboard that displays near real-time events. This dashboard integrates two cyber-intelligence feeds. One feed is from the National Association of Manufactures

(NAM) which furnishes industry vertical specific risks and vulnerability data. The other feed is the Department of Homeland Security (DHS) cyber risk feed.

At approximately Midnight Sunday, the UEI network begins to experience unusual traffic directed at the company's entire network address space, which is logged and packet captured. This traffic does not fit any known malicious signatures so no alerting is initiated. Absent of a rule or signature, some of this traffic is allowed to pass into the UEI DMZ. This traffic abruptly stops at 7:00 AM local. A pre-scheduled task of the Cybersecurity dashboards logging system prepares UEI's out of hours update feed to NAM and DHS for distribution using TAXI at 6:00 am. TAXI allows for the secure, authenticated, transfer of STIX data between trusted entities. UEI is required to share the data as a condition for receiving the NAM and DHS feeds at reduced cost. However, UEI is not concerned with this data sharing because the logging system obviewscate the actual organizational IP addressing data with the organization assigned "@idref" in the ExploitTargetType of the Exploit Target Schema within STIX. Since the actual event ID is from UEI is not altered, should a question arise about a specific event ID, only UEI can cross correlate the obviewscated data to the internal logging to identify the source and target systems. Only the UEI and DHS can correlate the "@idref" to the actual organization. This protects the anonymity of the UEI, allowing it to subscribe and share data among numerous entities without risk of identity exposure. DHS as the governmental issuer of US Identify Reference number, holds the organizational identity in escrow and agrees to not release the unique identity to organization correlation. Thanks to congressional passage of updated Cybersecurity sharing legislation, the organizations identity is protected under shielding law and is not publically disclosed in criminal or civil prosecution proceeding documents.

At 8:30 AM Bob, the UEI network security engineer, open the Cybersecurity dashboard for the first time that day and observes the traffic. Bob becomes concerned about the odd traffic that occurred the previous night. Normally, when his dashboard pushes a feed to NAM and DHS, it downloads any updated indicators at the same time from the prior submission. This allows him to control the traffic impact on the network from the dashboards information sharing services. Updates occur 3 times a day, which under normal circumstances, is the normal course of action for event updates. In this case however, his concern prompts Bob to force an update of the indication correlators to dashboard from MAN and DHS to see if any trending information is available. Several minutes later, the updates are downloaded and the dashboard is updated. This causes the dashboard to turn Red, indicating significant high-risk activity detection.

Using the dashboard Bob is able to quickly drill down into specific indicator details and determine that a malicious actor from China has scanned his network for a newly discovered vulnerability that allows for router transversal regardless of applied access controls. This was due to a cybersecurity analysts who identified the risk earlier in the evening and developed early detection indicators that when the STIX data is replayed now indicate and classify the probe. The analysts were tipped to the possible issue by STIX indicators from updates provided earlier in the day identifying odd traffic that required further analysis. As Bob reviews his updated results, he sees additional indicators that the attackers appear to be scanning for a specific SCADA controller that exists on his manufacturing floor. Armed with this information, Bob begins to coordinate with the UEI incident response team. Approximately 60 minutes after Bob discovers the issue, he receives a call from the DHS National Cybersecurity and Communications Integration Center (NCCIC) informing them they have detected a problem emanating from his network. Bob immediately conferences in his Incident Response leader and they document a series of actions requested by the NCCIC to be performed. These actions allow the UEI Incident

Response Team to preserve the intrusion data for national analysis. Later that day, using information securely uploaded via TAXI from UEI and other industry partners, a briefing to the Industry association NAM is provided. This briefing results in a bulletin regarding the attack being issued within the vertical. Simultaneously to the indicators being released, the DHS workflow releases information to the security vendor community identifying the attack, how the attack works, and known indicators such as strings, files, and system calls initiated. This leads to the release of firewall and anti-malware signatures later that evening. In a parallel workflow, this information being shared into the CybOX system, alerting other international network system managers to the issue, detection mechanisms, and mitigations as they become available.

In Summary: Bob's participation benefits his company in multiple ways. By leveraging a STIX compliant cybersecurity architecture, he reduces the management complexity of cyber operations through the use of an integrated cybersecurity dashboard. UEI enjoys lowered civil liability insurance cost through a measurable increase in due diligence associated with shorted detection timelines. UEI becomes a sensor on the global network that can share possible Indicators of Compromise (IoCs) while maintaining their anonymity. Collection of early possible indicators allow workflows that efficiently distribute potential risks to security engineers that can perform critical analysis earlier into the detection cycle. Faster identification of risk, vulnerabilities, and compromise indicators leads to faster development of attack patterns which are be more rapidly shared with cybersecurity vendors. With a more rapid sharing of IoCs, the viability of new risks across protected participating networks is dramatically shortened.