ACTRA – A Case Study for Threat Information Sharing

Jon C. Haass
Embry-Riddle University
3700 Willow Creek Road
Prescott, AZ, 86301
+1-928-777-6975
jon.haass@erau.edu

Gail-Joon Ahn
Arizona State University
699 S. Mill Avenue
Tempe, AZ 85281
+1-480-965-9007
gahn@asu.edu

Frank Grimmelmann
ACTRA, Inc.
2102 Encanto Blvd, MD 3900
Phoenix, AZ 85009
+1-623-551-1526
fgrimmelmann@actraaz.org

ABSTRACT
This paper provides a case study for information sharing within a public/private not-for-profit partnership organization called ACTRA – Arizona Cyber Threat Response Alliance, Inc.. This initiative is comprised of public and private entities, with government agencies as invited guests, aligned around the goal of improved response to cyber security events. Technical, political, legal and organizational issues arise when multiple parties attempt to exchange information in a formal setting. Benefits and specific solutions developed are discussed. The study concludes with several areas for future improvement and investigation, as well as recommendations for newly forming sharing groups.

Categories and Subject Descriptors
D.4.6 [**Security and Protection**]: Information and Data Sharing – *access controls, information flow controls, authentication* See also K.6.5. *Intellectual Property, Government Privacy and Ethics.*

General Terms
Security and Privacy

Keywords
TAXII; STIX; Cyber Threat Intelligence Sharing; ISAO; ISAC

1. INTRODUCTION
The conceptual benefit of sharing cyber threat information is at the heart of the current anti-malware industry led by companies such as McAfee and Symantec. Information sharing among different organizations without that same central provider has been evolving in pockets with the FS-ISAC (Financial Services Information Sharing and Analysis Center), formed in 1999, one of the earliest examples. The move from theoretical benefits to practical implementation of multi organization cyber threat information sharing remains a challenge. New Information Sharing and Analysis Organizations (ISAO) are being encouraged and partially funded by government initiatives under the Department of Homeland Security (DHS) in response to the Executive Order 13691 released February 2015.

Many organizations and participants today agree on why information sharing is important. In a recent report to Congress, the identified advantages included greater agility and situational awareness as well as a "deeper understanding of threat actors' tactics, techniques and procedures (TTPs)" [1]. If properly developed, shared information should lower the cost of defense and increase the ability to collaboratively discover compromised systems. A survey of IT professionals (not all of whom were in formal shared information networks) reported, however, that most of the threat information they received was not timely or specific enough (actionable) to meet their perceived need [2].

WISCS'15, October 12, 2015, Denver, CO, USA
 ISBN 978-1-4503-3822-6/15/10…$15.00
DOI: http://dx.doi.org/10.1145/2808128.2808135

Cyber security professionals are today primarily embedded in the IT organization though it is now clear that the impact to a company or organization goes beyond the classic bounds of the technical computer domain. Product information, business strategies, sales and marketing contact information, proprietary information, and legal documents stored electronically are supported by IT, but are fundamentally controlled and used by other organizations. Access to these, their linkage with email accounts, web applications and documents stored on a variety of platforms including mobile devices and cloud systems stretches the ability of an IT department to protect the data [3].

Furthermore, in the first version of the National Institute for Standards and Technology (NIST) cyber security framework, it is highlighted that access to threat information including TTPs is critical to the development and maintenance of a robust cyber security plan and implementation within an organization [4].

One of the goals of ACTRA and other ISAOs is to break down the resistance to information sharing and engage, not only the technical workers but also the business leadership. The high level management teams are best equipped to see the overall scale of risk and reward beyond just the direct cost of spending on cyber security. The success of information sharing requires the development of metrics that can be gathered, monitored, analyzed, and then effectively communicated to achieve improvement as well as to continue justifying the expense of the practice [5].

A number of potential models for effective information sharing have been proposed and begun, for example PRISEM in the Puget Sound region and ACSC in New England. It is the community of interest that must implement and investigate the results of corporate and government information exchange where the vast bulk of critical assets sought by adversaries reside [6]. Cyber crime, increasingly the work of large networks of individuals, is best countered with a similarly organized structure [7]. In other words, it clearly confirms that understanding and investigating cyber crime take *a Network to Defeat a Network*.

2. ACTRA FORMATION
ACTRA grew out of relationships developed with FBI's InfraGard and the Arizona Counter Terrorism Intelligence Center (ACTIC). The organization is incorporated as a nonprofit company with a board, a technical group of subject matter experts as well as an advisory board from private and public sector

entities. This structure divides along lines of business, policy and technology with interchange as needed to create a functioning solution for the different requirements of the constituents.

The ACTIC, formed in 2005, is a government sharing structure that was to address the challenges for timely exchange of intelligence and critical information among state, local and federal public safety agencies and ultimately provide a real-time information link with law enforcement and first responders [8].

ACTRA built on experience gained through the efforts to bridge tribal, state, local and federal agencies, added the dimensions of the public/private sector and support of academic interests. The foundation of the effort rests upon the desire to improve security without adding another layer of expense or process that would be a burden to members, resulting in a flat responsive structure that today operates in near real-time.

This regional, cross industry information sharing alliance provides the opportunity to have in person meetings creating trust that helps bridge organizational reluctance, and provide the cultural foundation. ACTRA today has grown to include 14 of the 16 designated critical infrastructure sectors as described in Presidential Policy Directive 21 (PPD-21) and is a model for a multi-sector, regional, and potentially nationally scalable solution [9].

3. CHALLENGES

In late 2012 there were few examples of cross sector cyber threat information sharing models, most were ad hoc and primarily point to point informal sharing among colleagues. Much of the success was hidden and below the approval radar of the organizations in which workers operated. However this type of activity does not scale nor can it be funded to become institutional. It may rely on single points of contact that could move to a different job position losing that valuable connection. ACTRA on the other hand was designed to be visible at the C level organization, as well as legal, to foster the needed support for the technology wizards that would ultimately have the challenge of implementation.

3.1 Organizational Issues and Concerns

Marketing and awareness was an initial hurdle and required communication via phone, email and at events in what seemed like a 24/7 campaign. C-Level executives were at first reluctant to enter into a new type of unproven relationship with potentially competitive organizations. Worse perhaps, what does it mean to share information with the government? In the past most people and companies sought to remain out of the range of government interaction and potential regulation or scrutiny.

Corporate members could benefit from classified or sensitive data available from government agencies. Sharing with other corporations can likewise provide coverage that no single company no matter the size can hope to access. Many companies are not practiced in the handling and dissemination of external data. Therefore, an important challenge is to address what the profit motive and accountability structure is.

Government entities enjoy certain protection from liability, however, they are at risk if classified data is shared in an irresponsible manner. This can compromise on going enforcement or surveillance activities and be costly in terms of lost efforts and use of government funds. Individuals can also be harmed in their careers should problems arise within their jurisdiction.

Another challenge is to build a common understanding on the role of academic members beyond the obvious special case of alignment as either a public institution or private entity. For researchers and students in the field of cyber intelligence and security, public policy and law, it is an excellent opportunity for research projects, study and hands on experience. At the same time, it is critical to fulfill security requirements in performing any projects and exercises with public and private entities.

3.2 Legal and Financial Matters

It was recognized from the outset that a template non-disclosure agreement (NDA) followed by a membership agreement was the best approach to meeting the legal requirements of the different organizations. As reviews occurred the template rapidly matured and was able to be operational within 3 months. This put the Alliance, formed as a nonprofit corporation at the hub of the communications since the agreement is with the Alliance not with the peers. This solved the potential nightmare in handling and maintaining exponential growth of agreements as the network grew.

Key to the relationship was the agreement to protect the names of members in the organization unless they were willing to be associated in a public manner. Some companies and organizations were concerned that they would become a greater target should they be identified as an active participant in information sharing.

It was also discovered that different types of members would be required in order to gain the advantage of disparate players. As will be further discussed in future work, this is an issue particularly for smaller organizations that may benefit from sharing yet can not participate fully for either technical or financial reasons.

One of critical questions in this area is “would there be increased liability for a company if it received threat information that was not promptly utilized?” This scenario is playing out in a recently settled court case with retail giant Target and its potential inaction in 2013 to vulnerabilities. The cost to a company in legal and financial fallout could be large. Faced with undefined risk, corporate members seek to limit their exposure with legal and policy choices that are being discussed in new legislative proposals. Also, not engaging in information exchange may itself create legal liability as standards evolve.

3.3 Technical Hurdles

As security organizations scramble to keep up with the ever-evolving threats, each organization develops its own methods and practices. Best practices differ by industry sector as well as by the size of the organization. Sophisticated and larger organizations with strong technical cyber security teams utilize network monitoring, intrusion detection and other management tools. These can integrate external threat data in manual or even automatic modes. The mechanism for translating threats into a standard format and framework has improved but is still in an early stage. The decision to utilize STIX and TAXII as the interface puts a burden on less able or resourced organizations [10]. There is additional potential risk in connecting networks even if the reason is for the sharing of sanitized indicators. This is mitigated by implementation of appropriate internal processes.

4. SOLUTIONS AND BENEFITS

ACTRA was able to build on developments and experiments from other sharing organizations, such as the ISACs and government inter agency experiences, thanks to the broad skill set of the different invested participants. Even so, solutions necessarily

have evolved and will continue to shift. As more organizations join, the tools and techniques will mature, and international considerations and preferences will come into play.

It was recognized that information was valuable on different time scales. The ideal state is for a threat or vulnerability to be discovered rapidly, characterized and communicated in a timely and actionable manner. As taken from Verizon's 2013 study on data breaches shown in Table 1, this desire does not match well with the reality of cyber threats [11].

Table 1. Time scale disparity: compromise vs discovery; the fraction of breaches and the time to damage and discovery.

Timescale	Minutes	Hours	Days	Weeks
Damage	23%	60%	13%	3%
Discovery	1%	9%	11%	78%

Damage is done in seconds, minutes, and hours while discovery and containment are more often measured in days, weeks or even months. Of course it is possible that the early stages of reconnaissance and planning are also on a longer time scale. These activities are today not visible. This issue points to the leading edge of cyber security research – what tools and techniques can close this gap? Is information sharing in the form of a larger but more loosely coupled information gathering honey net coupled with intelligent mining and pattern analysis able to shift the advantage; this is a research recently begun in ACTRA.

4.1 Situational Awareness – White Papers

At the policy and educational level, ACTRA has been successful in raising awareness in the highest levels of organizations. These products provide insights, best practices, and tips for improving awareness among the users within an organization. One example is a debrief on some of the valuable learning from the recent incident where a corporation such as SONY was targeted by a nation state level threat actor with intent to damage not just gain financially or exfiltrate intellectual property. The papers are appropriate to the slower time scale and meant to be consumed via email. Their impact is on policies and procedures, offering a reminder to practice and keep frameworks alive and changing.

Based upon comparisons within ACTRA, teams that have a clear response plan and procedures, and most importantly practice disaster scenarios, are better able to handle actual situations. Sharing of these best practices, backup and recovery techniques and example plans has been rated very useful.

Companies are also re-packaging threat information and white papers, providing a version as educational outreach to include the "end user" in the cyber security defense plan. Data inputs for enriching threats intelligence is also available through outreach via "crowd sourcing". This changes it from some abstract item to a current and actual example.

4.2 News and Blog Site

ACTRA has developed an invitation only site to allow members to access information on their schedule having been alerted, rather than push via email. A user can then request notification when a new entry of interest is posted. Information is categorized based on the survey responses for types relevant to the member. The site has an editorial board and a process for creating articles, alerts, and intelligence briefs. Members can also contribute posts or comments. This is successfully utilizing university students to seek relevant material via open source (OSINT) methods, which provides an excellent experience for the students and a cost effective resource to the Alliance.

4.3 Alerts

More actionable and timely are the official use only alerts including FOUO information with specific data from on-going investigations, analysis or active threats or events. Though these may still be less effective compared to the actual initial breach, it is early in the analysis lifecycle so not all attribution or analysis is available. Examples include potential IP addresses, web addresses, code samples, and hash signatures associated with a specific known event. This can be utilized by an IT organization to update firewall or intrusion detection systems (IDS) rules, compare with logs from their own organization network feeds and potentially create additional data from their early alert. ACTRA disseminates these in both classified and un-classified settings through its vetted and pre-trusted relations.

This is one of the more sensitive types of communication as it represents information that, if leaked, could alert the attacker of the ability to identify possibly causing them to go underground, change their TTPs or accelerate plans with any existing campaign. ACTRA has created limited distribution lists, and the efforts are rated as beneficial by recipients. They would like to see more timely and actionable alerts and this is an area of growth, and the expansion of threat intelligence data feeds.

Separate classified briefings are held with invitation only and pre-registered list used to validate attendees. This met the security needs of the public agencies as well as provided greater access to intelligence to the private sector participants.

4.4 Automated Data

The most exciting development is the acquisition and dissemination of threat data that is closer to real time based on information gathered from IDS, security information and event management (SIEM) solutions and investigations. The goal of this work is to achieve a machine to machine connection that can be used along with other threat intelligence data in the security operations center of member organizations seamlessly integrated with requisite process flow. The groups have agreed to utilize the DHS/MITRE specifications of STIX/TAXII initially. Vendors are supporting the import of this type of data and the specifications are being advanced through the standards development organization OASIS. The Alliance members' implementation is still in the early stages. Those participating members indicate a strong interest in continuing and rate the value of the effort as high.

The most successful operational efforts occur from member to member threat incident exchange that can include zero day events. In the past month automated feeds have come on-line supplementing the existing 30,000+ indicators of compromise (IOCs) already available to members, the majority at this time derived external to the member organization. The key critical component to the members is to insure that the content delivery is carried out in a secure manner. Hence, it ensures that operational security focuses on protecting information on specific TTPs, to avoid educating attackers.

4.5 Survey on Benefits

In the early stage of ACTRA formation, a survey was developed to understand what kinds of information would be valuable, who the expected audience was and how the data should be delivered. This helped to develop the products and organize the Alliance. The results were consistent with larger surveys [12] and the survey included some questions to allow correlation. One of the results found was that top leadership, including the board, is

generally uninvolved. This was important in the decision to target the C-level of member organizations with appropriate materials.

The area of greatest interest by the survey respondents was support or intelligence on advanced persistent threats (APT). This has been a focus for the think tank group within the Alliance and remains an area of future growth. New tools and incident management systems appear promising, and more are supporting the chosen emerging exchange standards and formats.

A new follow up survey to assess how the Alliance has performed in meeting the expectations of its members has begun. The full results of that new survey, though not available yet, will help guide new focus over the next year. Early indications point to continued technical and resource investment in ACTRA, a desire to connect with other organizations and enhancement of the real time components.

5. FUTURE EFFORTS

Continued operations and enhancement of the present set of offerings point to a change in the predominantly-member driven volunteer model. The ability to deliver products in a timely and predictable manner requires evolving accountability. An aspect of this was apparent in the predominance of larger corporations among the members. Smaller organizations cannot spare their already limited resources on a regular basis. The organization is looking at a variety of different solutions, as well as seeking other funding sources to expand the core team.

As seen in recent security breaches and reported in surveys, smaller companies in the supply chain have been targeted as means to access ultimate higher value assets. It is critical to include smaller mid-level members of the supply chain in future initiatives, and this has begun with educational efforts in cooperation with the Arizona Tech Council. The success of using students to provide OSINT capabilities, create reports, develop material for and manage blog sites and newsletters will be continued by ACTRA and key stakeholders. An initiative to provide internship and co-op opportunities will allow a more reliable access to this resource particularly in the summer months. Funding from grant programs and the awareness of the workforce growth opportunity for companies will further assist this development.

An area of research includes identifying characteristics of shared data to help reduce false positives. This is related to another topic to be explored the identification of "critical" indicators.

Experience with member companies and academic researchers has earned trust and it is planned to make more data available for testing newly developed algorithms and concepts, with appropriate security precautions and non-attribution. An area of interest is creating weight methods to validate threat indicators derived from different sources. This is relevant when the sources have different methods, practices and standards for inclusion in the set. This has similar goal as certification done by TF-CSIRT.

This points to a variety of desired improvements in the data sharing platform as companies and vendors learn better the methods and automation to transform internal threat data into a sanitized (privacy preserving) exchange format.

6. CONCLUSIONS

With over two years as an organization, ACTRA continues to grow in membership and scope of its offerings. Even though some participants expressed their disappointment that progress was not even more rapid given the time investment, this case study clearly indicated the importance and necessity of the systematic procedures, framework and cultural development that can facilitate threat information sharing. Information sharing, like the popular social networking activity, is a group activity and requires active and frequent engagement for proactively coping with security threats and exploits in a timely manner. Based on discussions with members, multi-sector sharing improves threat visibility beyond the single sector focus of the more traditional ISAC model. The distinction may disappear as more trusted connections are created and sharing technology and policy improves.

Recommendations: Other ISAOs could benefit from the experiences gained over the course of ACTRA early stages: 1) Establish expectations and set realistic goals with at least semi-annual review of progress; 2) Allow for changes in the plan, admitting when adjustments are required; 3) Create an atmosphere of transparency and inclusion; 4) Develop a core team and leadership that is willing and able to meet regularly and often; 5) Establish alternate representatives to maintain continuity; and 6) Create a communication method for decisions, issues and suggested solutions.

7. ACKNOWLEDGMENTS

Thanks to the members, core team, board and the subject matter experts of ACTRA that participated in interviews and dialogue. Evelyn Brown, Embry-Riddle University Cyber program student, provided valuable assistance in research and survey development.

8. REFERENCES

[1] Lewis, J.A., and Zheng, D.E., March, 2015, *Cyber threat information sharing recommendations to Congress and the Administration*. A report of the Center for Strategic and International Studies.

[2] Ponemon, April 2014. *Exchanging cyber threat intelligence: there has to be a better way.* Ponemon Institute Research Report, Ponemon Institute LLC.

[3] Peretti, K., 2014. *Cyber threat intelligence: to share or not to share.* Privacy and Security Law Report, Bureau of National Affairs.

[4] NIST 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.0. National Institute of Standards and Technology. Accessed at: http://www.nist.gov/cyberframework/.

[5] Fleming, M. H., Goldstein, E., and Roman, J. January, 2014. *Evaluating the impact of cybersecurity information sharing on cyber incidents and their consequences*. Homeland Security Studies and Analysis Institute.

[6] White, G. and Zhao, W., 2014, *Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security,* System Sciences (HICSS), 47th Hawaii International Conference on, pp.1987-1996.

[7] Zhao, Z., Ahn, G.-J., Hu, H. and Mahi D. 2012, *SocialImpact: Systematic Analysis of Underground Social Dynamics*, 17th European Symposium on Research in Computer Security (ESORICS), Pisa, Italy.

[8] ACTIC, 2005. Accessed at: azdohs.gov/Councils/acticoc.

[9] Presidential Policy Directive – Critical Infrastructure Security and Resilience, PPD-21, 2013. Accessed at: https://fas.org/irp/offdocs/ppd/ppd-21.pdf

[10] Barnum, S. 2013. *Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX)*. The MITRE Corporation.

[11] Verizon, 2013. *Data Breach Investigations Report.* Accessed at: http://www.verizonenterprise.com/DBIR/

[12] PwC, 2015. Global State of Information Security 2015. Accessed at: http://www.pwc.com/gsiss2015.