Trust and Collaboration to Enhance Cybersecurity*

Keman Huang, Keri Pearlson, Stuart Madnick

December 14, 2017

This paper is written to explore the relationship between trust and collaboration as they relate to cybersecurity. It has been our observation that cybersecurity is enhanced when entities collaborate with each other, and collaboration is most effective when trust is present. One example of collaboration between entities is the Information Sharing and Analysis Centers (ISAC).

Trust for the Supply Chain

There are three Prevalent Assistance Process between the customer and supplier to build trust along the supply chains [1] when pecuniary incentives cannot be fully aligned:

1) **Information Sharing**: supplier provides the customer with relevant information, which the customer may consult when making her decision;
2) **Advice Provision**: the supplier recommends a decision to the customer, and the customer decides whether and to what extent she will follow the recommendation
3) **Delegation**: the supplier makes the actual decision on the customer's behalf, while the customer determines beforehand the set of decisions that the supplier is permitted to make.

These assistance process will impact the customer's and supplier's motives that give rise to trust and trustworthiness and then affects the level of cooperation and payoffs. Considering the effectiveness for trust building, the information sharing leads to the highest trust and trustworthiness and then advice provision while the delegation performs the worst.

Cultivating Trust in Virtual Communities

Trust plays an important role for the virtual communities to customers, which can be reflected by the member's belief in the sponsor's benevolence, integrity, and judgment. The following components are critical for the trust cultivating [2]: a sponsor makes efforts to provide quality content, foster member embeddedness are important to improve the member's belief about a sponsor's sense of shared values with and respect for community members, which then cultivate the trust between the sponsor and members. This trust will further improve the member's willingness to share personal information, cooperate in new product development efforts, and loyalty.

Note that the research also shows that a member's perception that a sponsor makes efforts to encourage interaction have no significant benefit to construct the trust among members.

Information Sharing for Cybersecurity

Based on the deep analysis about the institutional cyber security landscape consists of a complex array of organizations that exhibit significant diversity with regard to missions, mandates, interests, opportunities, and constraints. we can get the following observations [3]:

1) The information technology-sustainable development linkage has become an integral feature of the international community's policy priorities.
2) The current institutional landscape resembles a security patchwork that covers critical areas rather than an umbrella that spans all of the known modes and sources of cyber threat.
3) Given the multiple contexts and diverse institutional motivations, we expect that responses will be driven more by institutional imperatives and reactions to crisis than by coordinated assessment and proactive response.
4) Due to the complex global agenda at all levels of development, states may not be willing to proceed until international norms are developed, rather they will 'take matters in their own hands' and develop first order responses.
5) Cross-sector collaboration among public, private, and volunteer organizations may serve as a temporary measure to cover holes in the current defense network. However, at some point effective institutions will be necessary; they may develop in parallel with rising public awareness.
6) So far, we have not yet seen large terrorist groups engaged in intense cyber malfeasance. This pattern cannot be expected to continue. Efforts to infiltrate critical US infrastructure and the devastating attacks on Estonia and Georgia in 2007 and 2008 underline the dangers of being lulled into a false sense of security. As the Internet becomes increasingly central to modern society, it is likely that criminals, terrorist groups, and other opponents to state authority will target this sector in the hopes of disrupting critical national functions. So far, the potential for significant threats is far greater than institutional capabilities to contain these threats. In other words, the 'demand' for security far exceeds the provision of effective "supply."

Incentives and Barriers for Cybersecurity Information Sharing

More practically, though many information sharing organizations were created, a number of drivers and challenges have emerged that either incentivize or deter firms from participating in cyber information sharing organizations. The survey among (IC)3 members, SIM CyberSecurity SIG members, and other CISO contacts, where the target participants were CISOs or other individual's working in a firm's information security office with knowledge of their firm's membership in cybersecurity information sharing organizations (25 response) shows that [4]:

• Not enough sharing is occurring in small businesses, whereas large businesses to a greater degree are sharing and engaged
• Firms are not joining cyber information sharing organizations primarily because they are not gaining value out of the information those organizations provide, or don't see the value in the type of information the organization is offering to provide to its members. Secondary reasons include the inability to manage additional information processing. For small businesses, the cost of membership for joining an information sharing organization serves as an additional barrier.
• Inability to consume data feeds due to limited resources in financial or people resources, is considered as the greatest organizational challenge impacting their firm's decision to not join or terminate a membership in a cyber information sharing organization
• Non-members of any sharing organizations view industry specialization as the most important characteristic, followed by low cost of membership, broad membership profile, and no requirement to share information. Current members of sharing organizations view a broad membership profile as the most important characteristic, with industry

specialization and no requirement to share information as equally important, and a low cost of membership as the least important.

- In order for a sharing organization to be effective in gaining and maintaining members, as well as operating effectively, it should have some agreement that maps out the relationship to help establish trust.

Information Sharing and Analysis Centers

On May 22, 1999, Presidential Decision Directive-63 created the concept of Information Sharing and Analysis Centers (ISACs) to help critical infrastructure industry players protect their facilities, personnel and customers from cyber and physical security threats. Today, there are 24 operating ISACs, where Financial Services ISAC (FS-ISAC) is considered as the most successful. Today, the FSISAC has 1000s of members. Please refer to [4] to see some more detail comparison between Financial Services ISAC (FS-ISAC) and Information Technology ISAC (IT-ISAC).

One important perspective for FS-ISAC is that the Financial Services ISAC not only sends and receives information about threats and vulnerabilities through an automated feed to/from its members, but also publishes security best practices and holds trainings, workshops, webinars, and special events to provide members with better cyber situational awareness. The most recent activity from FS-ISAC is that the FS-ISAC unveiled its "Sheltered Harbor" initiative [5] — an industry effort to improve sector-wide resilience in the face of a cyberattack on November 22, 2016. Sheltered Harbor intends to create an extra layer of protection against potential significant cyber risk. Specifically, Sheltered Harbor enables financial institutions to securely store and rapidly reconstitute account information, making it available to customers, whether through a service provider or another financial institution, if an institution appears unable to recover from a cyber incident in a timely fashion.

Over all, no defense is foolproof. "Such efforts have had mixed success in the past" while the risk that the backups are comprised also need to be considered [6]. Many more efforts are necessary.

Collaboration to proactively defend against Cyber Attack

The public-private partnership is important to defend against the cyber threat and different actors need to work together to build a safer connected world. However, the externalities, misaligned incentive and the information asymmetries result into market failures and raise the necessary for the comprehensive framework to allocate responsibilities to different parties so cybersecurity can be improved in the places where economic forces disincentive it. Based on the understanding of the cyber threat, especially in the cyber attack as a service context, we develop a framework [7] to identify the responsibilities and actions falling to different actors based on whether the actors have the capability to take the actions. It reveals the potential to disrupt the cyber attack capability supply chain, enable an "attack-back" perspective, to reduce the threats from cyber space.

In addition, it can be seen that the public sector plays an important role to defend against the cyber threat. Not only provide the protection capability for the private sectors, especially for the small businesses who don't have the resource to build their cyber security capability, the public sector should also involve into this proactively defend efforts to disrupt this cyber attack business supply chain.

References

[1] Özalp Özer, Upender Subramanian, Yu Wang (2017) Information Sharing, Advice Provision, or Delegation: What Leads to Higher Trust and Trustworthiness?. Management Science

[2] Constance Elise Porter, Naveen Donthu, (2008) Cultivating Trust and Harvesting Value in Virtual Communities. Management Science 54(1):113-128.

[3] Nazli Choucri, Stuart Madnick, Priscilla Koepke, "Institutions for Cyber Security: International Responses and Data Sharing Initiatives" at http://web.mit.edu/smadnick/www/wp/2017-06.pdf

[4] Priscilla Koepke, Stuart Madnick, Keri Pearlson "Cybersecurity Information Sharing Incentives and Barriers" at http://web.mit.edu/smadnick/www/wp/2017-13.pdf

[5] FS-ISAC and Sheltered Harbor, https://www.fsisac.com/sites/default/files/news/SH_FACT_SHEET_2016_11_22_FINAL3.pdf

[6] Prof Stuart Madnick quoted in the Wall Street Journal – "Banks Build Line of Defense for Doomsday Cyberattack", December 3, 2017. https://www.wsj.com/articles/banks-build-line-of-defense-for-doomsday-cyberattack-1512302401

[7] Keman Huang, Michael Siegel, Stuart Madnick, "Cybercrime-as-a-Service: Identifying Control Points to Disrupt", http://web.mit.edu/smadnick/www/wp/2017-17.pdf