MIT MANAGEMENT
SLOAN SCHOOL

INTERDISCIPLINARY
CONSORTIUM
for IMPROVING
CRITICAL
INFRASTRUCTURE
CYBERSECURITY
(IC)³

Cybersecurity Information Sharing Incentives and Barriers

Priscilla Koepke

Working Paper CISL# 2017-13

June 2017

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Cybersecurity Information Sharing Incentives and Barriers

June 2017

Priscilla Koepke
Sloan School of Management, MIT
pkoepke@mit.edu

I. Introduction

Increasing attention is being paid to the importance of gathering, analyzing, and sharing information as a key factor to improve computer security. As cyberattacks have become increasingly ubiquitous, in parallel we've seen the number of cyber information sharing organizations also proliferate. From what began as the Computer Emergency Response Team Coordination Center, CERT-CC, created in response to cyber threats in the late 1990s, has today grown to a network of over 351 recognized CERTS, as well as a number of international cyber coordination organizations both government and private sponsored, and 24 sector-based information sharing and analysis centers, ISACs, with domestic and international reach. Many of these organizations, particularly the ISACs, share security best practices and solutions with members, encouraging mutual collaboration, while also aiming to build trust between networked environments of similar institutions. The goal is to make sharing information more likely.

Since many of these organizations were created, a number of both drivers and challenges have emerged that either incentivize or deter firms from participating in cyber information sharing organizations. This paper examines these drivers and challenges, referred to as incentives or barriers, as they relate to cyber threat sharing. Through a literature review of research that first addresses information sharing more broadly, and then focuses on cyber information sharing, I outline the major incentives and barriers to sharing cyber threats today, building a framework to better understand what is either encouraging or impeding sharing efforts. With the growing need and importance of sharing information about cyber threats, understanding how to better align the benefits and minimize the costs of sharing is a critical step forward.

II. Incentives

The incentives that encourage information sharing of cybersecurity data can be divided into eight categories, identified and described below. Each of these categories is multi-faceted with various subcategories, but for the purpose of this paper have been organized into more general categories for research and analysis.

A. Situational awareness

Many firms share information about cyber threats and vulnerabilities because it enhances their own situational awareness. This awareness not only helps firms better assess vulnerabilities, but improves their analysis and production capabilities. Building situational awareness of their cyber environment helps firms to better prevent, protect, mitigate, respond to, and recover from threats and attacks.

B. Legal Protections

Over the course of the last few years, legal protections have been enacted to protect firms from liability if they share cybersecurity data. The various legal protections include Antitrust Law and FOIA exemptions, civil and enforcement liability shields, government restrictions on the use of information, and policies and standards to protect PII/IP. These protections not only assuage company fears of accountability, but also encourage firms to participate in sharing efforts by reducing the risk of sharing.

C. Technological

A variety of technological incentives exist that encourage firms to share cybersecurity information. The first is if the sharing language is simple and efficient, fosters uniformity, and creates clarity. Common standards, vernacular, and technology specifications act as important incentives to share, so if the platform for acquisition, access, retention, production, use, management, and sharing of information is built to promote these language characteristics, sharing is generally more likely to occur. Second, sharing automation capabilities also encourage firms to share because automation anonymizes the identity of the submitter, minimizes the amount of data collected, retains information for a limited time, and ensures information is used for authorized government purposes. Moreover, automation is fast and efficient, and creates a trusted environment and platform for exchange.

D. Costs

The sharing of cybersecurity information is can often decrease security expenditure costs, which then incentivizes firms to continue and increase sharing efforts. Sharing information has been seen to reduce costs and increase productivity because sharing and receiving information about cyber threats and vulnerabilities can reduce security expenditures, and reduce the number of needed security analysts needed. Sharing can also decrease the time needed to remediate after an attack, thus decreasing costs associated with incident response. This is due to the collaborative nature of sharing and the exchange of knowledge and expertise.

E. Management

Management incentives include governance flexibility with regards to information sharing relationships between people, firms, and organizations. Senior management's support of information sharing efforts and resources needed to facilitate sharing also serve as an incentive.

F. Informational

Informational incentives are divided between the process of sharing and the quality of information shared. A relationship that engenders a multidirectional flow of information, or reciprocity, serves as a significant incentive for firms to continue sharing cybersecurity information. Moreover, if the information received is actionable, reliable and relevant, firms will also be encouraged to share. Both create a mutually beneficial relationship and discourage free-riding.

G. Performance

Performance incentives are those that result from the routine execution of sharing cybersecurity information. The first incentive is an improved public image or reputation of the sharing firm as a result of its acknowledged efforts to build security awareness and better protect customer data. In some cases, an improved image could positively affect the demand for a firm's products. In this case, sharing could also augment the firm's stature within the sharing community, lending itself to serve as system-wide champion. In addition, participating in sharing efforts can enable firms to make better risk-informed decisions, which can lead to generally better firm performance.

H. Collaborative

Collaborative incentives include improved access to other organizations, agencies, and companies, which fosters expertise, knowledge, and expanded professional networks. Some firms are incentivized to join information sharing organizations to gain access to information from government, law enforcement or security services, which is not available from other sources. Trust and strong partnerships with the recipients or other collaborative members is also a major incentive to share. Lastly, an organizational network that is perceived to be low-risk by the firm can additionally encourage information sharing.

III. Barriers

The shortcomings that hinder information sharing of cyber threats can be divided into eight categories, identified and described below. Many of these challenges are complex and inter-related, but have been categorized for the purpose of research and analysis.

A. Constitutional / Legal

Constitutional and legal barriers often prevent firms from sharing information about cyber threats and vulnerabilities. Shortcomings in this area include privacy concerns, as legal protections that mitigate the sharing of PII/PI and competitive information are not considered comprehensive or strong enough. Many firms are also impeded from sharing due to concerns about the risk of disclosure of trade secrets, potential legal liabilities and actions that may be taken following the disclosure of cyber threats or attack details, and reputational damage that ensues from these disclosures.

B. Technological

Technological barriers include a lack of interoperability or compatibility between the sharing organization and firm. In some cases, organizations do not use a common language, such as TAXII or STIX, to share information about threats and vulnerabilities, but rather create their own sharing language that has not been widely adopted, making sharing increasingly difficult. Without a sharing language that is simple and efficient, fosters uniformity, and creates clarity, sharing is often constrained. Moreover, the complexity of information also acts as an impediment to sharing because the firm does not have the software or hardware capabilities to digest the information being shared, thus making it inoperative.

C. Informational

Too much shared information and a firm's inability to process this data acts as a significant barrier. This informational barrier makes finding valuable data hidden in a sea of irrelevant noise increasingly difficult to manage. These barriers often include challenges such as unreliable data, the impertinence of information shared, and difficulties of validating data quality.

D. Collaborative

Collaborative barriers include the challenges of establishing trust between a firm and sharing organization; the process complexity of sharing information; the size of the group information is being shared with; the type of participants receiving the shared information; and a lack of reciprocity from other stakeholders or the problem of free-riders. This barrier category also includes the risk of sharing with rivals/competitors who may use the shared information to enhance their competitive position.

E. Managerial

Managerial barriers involve challenges around the management of data and relationships from the firm and cyber information sharing organization perspectives. From the firm perspective, these barriers include internal managerial risk aversion and mistrust, often discussed as exposing the firm to "uncontrolled" risks, thus impeding the sharing of information. This managerial barrier could also be called loss aversion, leading to a status quo bias of not doing any more than already is being done. Barriers from the perspective of the sharing organization include the challenges of having no agreement recognizing a single, common centralized authority for establishing trust channels to exchange information between a firm and organization, and a poor management of shared information.

F. Organizational

Organizational barriers to sharing information include a firm's inability to consume data due to limited resources, and an absence of mechanisms to govern and control the use of sensitive information.

G. Performance

Performance barriers are those problems that result from routine execution of sharing information. Problems in this category include reputational damage and a loss of customers or revenue following an exposure. All these things yield a negative impact on a firm's performance, thereby impeding future sharing.

H. Cost

The costs associated with sharing information about cyber threats and vulnerabilities often serve as a significant barrier. Costs include the expenses associated with needing system technologies to share and receive information, which may have a high cost for some firms. Many firms also have limited human resources to process shared data and information, so there are costs with the need to hire more personnel to handle this type of analysis. In addition, barriers in this category include the cost of false positives based on outdated and/or unreliable data provided by a cybersecurity information sharing organization.

IV. Initial Framework and hypothesis

In order to examine the incentives and barriers to sharing cyber threats between firms and cybersecurity information sharing organizations, the project began by building a framework (described above) that identifies eight incentives and eight barriers. The framework was assembled based on interviews and a literature review of articles on related subjects. Based on this framework, we hypothesized that:

- The barriers are greater than the incentives, which is why not enough sharing occurs;
- Information sharing increases with firm size and industry size;
- Firms are more likely to share information with sharing organizations that have larger memberships
- In order for sharing to happen, the information shared must be timely, relevant, and of good utility and quality;
- Legal barriers are the greatest deterrent to sharing cybersecurity information;
- No matter the level of risk in a sharing relationship, trust is imperative in order for sharing to occur.

One of the goals of this research was to test these hypotheses and see to what degree each of these hypotheses prove true or false, and to get a deeper understanding of which incentives and barriers are having the greatest impact, and why. This would help identify why sharing of cybersecurity information is a challenge, help pinpoint where to focus future research to mitigate challenges, and how to take advantage and promulgate the appropriate incentives. These insights would give CIOs and CISOs a better way to categorize and understand the barriers and incentives for their firm, and help them understand potential benefits of joining an information sharing organization. It would also help cybersecurity information sharing organizations better understand what motivates and prevents firms from sharing, and how they could best structure their organization to provide the most benefits with lowest costs.

V. Analysis of survey respondents

To gain a deeper understanding of how incentives and barriers influence firms to share or not share information with cybersecurity information sharing organizations, as well as test the framework and hypotheses, a survey was conducted from April 27-May 18, 2017. The survey was distributed to (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. The survey received a total of 25 responses.

Some basic demographic information about the organizations surveyed include:

- Industries: 12 including, software publishing and internet services, healthcare, government, banking and financial services, insurance, professional services, transportation, pharmaceuticals, media and entertainment, education, and telecommunications.
- Size or organization: Small < 1,000 (11), Medium 1,000 to 9,999 (5), Large -> 10,000 (9)

The survey questions were designed to gather more information about the characteristics that incentive firms to share and the barriers that discourage firms to share, based on the developed framework discussed above. To do this, the survey's first section focused on firm's memberships with cyber information sharing organizations, and the reasons why they are members or not members of these organizations. The second section focused on the type of information that firms share and receive from sharing organizations. The third section focused on firm's behaviors and perceived barriers or incentives to sharing, where questions served as proxies to measure how impactful certain incentives or barriers identified in the framework are for respondents.

The results of the survey on a section by section basis are reviewed below.

Membership Characteristics

Who is a member in a cyber information sharing organization

The first step in understanding a firm's behavior and perceived barriers or incentives to sharing is documenting whether they are members of cyber information sharing organizations. The question asked was:

> Is your firm a member of any cybersecurity information sharing organization(s)?

The results of the question yielded 64% of firms which are not members of any information sharing organizations and 36% of firms which are members. These results tell us that there are more firms which are not members than firms which are members of cyber information sharing organizations.

The top-line hypothesis for this research was that "not enough sharing of cybersecurity information is occurring" in industry between different stakeholders. The results of the survey emphasize this hypothesis. While this insight is important, it's also critical to better understand the demographics of those firms that share versus those that don't share. The results of this analysis are shown in **Figure 1** below.

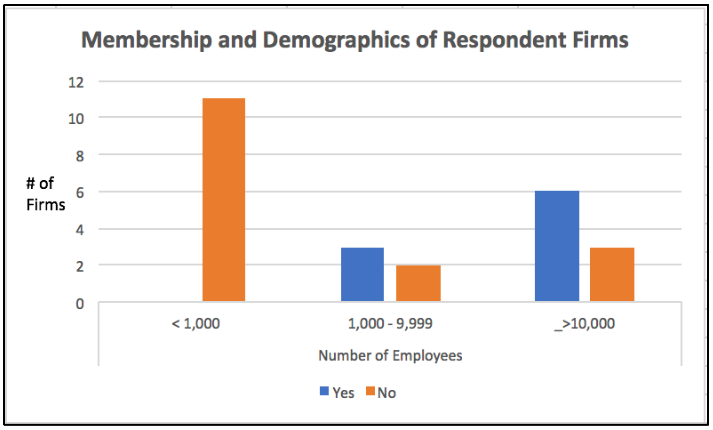

Figure 1

From **Figure 1**, we can see that the majority (67%) of firms that are members of at least one cyber information sharing organization are large firms with more than 10,000 employees. On the other hand, of those firms that are not members of any cyber information sharing organizations, the majority (69%) are small companies with less than 1,000 employees.

As a result, the first hypothesis should be approached with the caveat that not enough sharing is occurring in small businesses, whereas large businesses to a greater degree are sharing and engaged.

The second hypothesis approached in this research was that "Information sharing increases with firm size and industry size." The responses illustrated in **Figure 1** tell us that the bigger the firm, the higher likelihood it is a member of a cyber information sharing organization, which supports this hypothesis. In fact, research has shown that small businesses tend to have less security measures in place to protect against cyber-attacks as compared to large companies, and joining a cyber information sharing organization is one method to build a firm's defenses against cyber threats and vulnerabilities.

Of those respondents who said they are members of cyber information sharing organizations, they identified the following cyber sharing organizations in which they are members:

- MS-ISAC, NH-ISAC, Cyber Health working group, Infragard, NYSIC CAU, ThreatStream, Symantec MATI, Deepsight, Advanced Cyber Security Center, NSIN-based government collaboration forum

Behaviors of firms that are members of cyber information sharing organizations

For those firms that responded that are members of at least one cyber information sharing organization, the survey next asked questions to assess the interactions of these firms with the organizations they listed. The first question asked:

> How often do you engage with the cybersecurity information sharing organization(s) you listed above? Engagement could include participation in meetings, webinars, conference calls, etc. If you listed multiple organizations, please chose the frequency with the one organization that you engage the MOST.

The results tell us that:

- 40% engage with the sharing organization daily
- 40% engage 1-3 times a week
- 20% engage 1-4 times a month

A follow-up question asked:

> If you listed multiple organizations, please circle the frequency that describes your engagement with the organization with which you share information or engage with the LEAST.

The results tell us that:

- 25% still engage daily
- 75% engage 1-4 a month

From these two questions, we can assess that firms are engaging relatively frequently with the cyber information sharing groups that they are members. Not one firm selected the options of 'once every quarter' or '1-3 times a year.'

The survey next queried whether firms pay for membership by asking:

> Do you pay for membership in any of the cybersecurity information sharing organizations you listed above?

The responses tell us that 50% pay for membership and 50% do not pay for membership.

Finally, members of these sharing organizations were asked about the length of their membership. The following two questions asked:

> 1. How long has your firm been a member of the cybersecurity information sharing organization(s) you listed above? If you listed more than one organization, please focus on the one with which you have had the longest relationship
> 2. Has you firm left a cybersecurity information sharing organization at any point within the last 5 years?

Of those firms that are members of sharing organizations, 67% have been a member for 1-5 years, and 33% have been a member for more than 5 years. Within these relationships, 95% have not left a cyber information sharing organization within the last 5 years. This likely indicates that these firms have found their membership beneficial and feel the benefits outweigh the costs.

Why not members of a cyber information sharing organization

The next step in understanding a firm's behavior and perceived barriers or incentives to sharing is understanding why firms are not members of any or any other cyber information sharing organizations. The next survey question asked:

> Why have you not joined other / any cybersecurity information sharing organization(s)?

The results of this question are segmented into those respondents who reported they are members versus not members of cyber information sharing organizations, as illustrated in **Figure 2**. Overall, we see that the majority cite "Lack of information quality, utility, and value" as the reason why they haven't joined other or any sharing organizations. Of those who are not members of any sharing organizations, 38% selected "other" as their reasons why, citing they don't know of any sharing organizations, they didn't receive responses from organizations, or their firm is in Chapter 11. Other reasons were not provided.

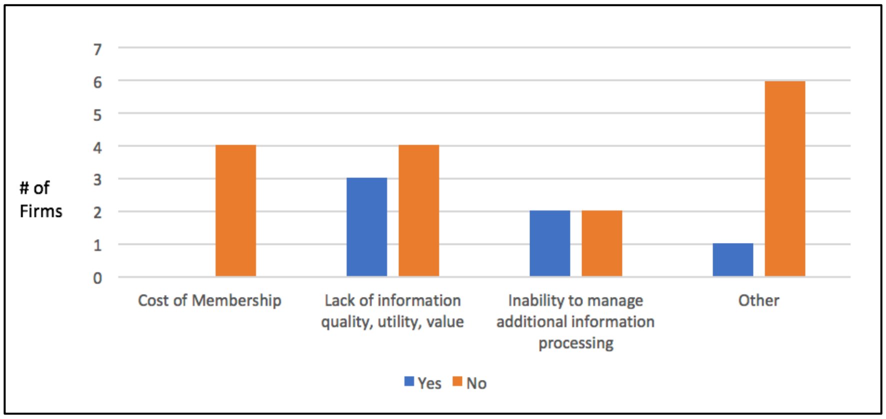

Figure 2 – Why Firms Don't Join Sharing Organizations

From **Figure 2**, we can assess that 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.

Furthermore, to better understand the organizational challenges that might be inhibiting firms from joining information sharing organizations or may cause a firm to terminate a membership in one of these organizations, the next question asked:

> Which organizational challenges most impacted or would impact your firm's decisions to not join or terminate a membership in a cybersecurity information sharing organization?

The results of this question reveal that 40% view the "inability to consume data feeds due to limited people resources" as the primary organizational challenge inhibiting a firm's ability to join cyber information sharing organizations. Examining **Figure 3**, the results show that this is particularly salient for those firms which are not members of any sharing organizations. Further analysis shows that of these firms which are not already members, and selected people resources as their greatest organizational challenge, 71% are small businesses, supporting research that shows small businesses lack proper defenses due to human and financial resources.

By grouping limited financial and people resources into a combined category called "limited resources," we find that 60% of respondents consider their inability to consume data feeds due to limited resources as the greatest organizational challenge impacting their firm's decision to not join or terminate a membership in a cyber information sharing organization.

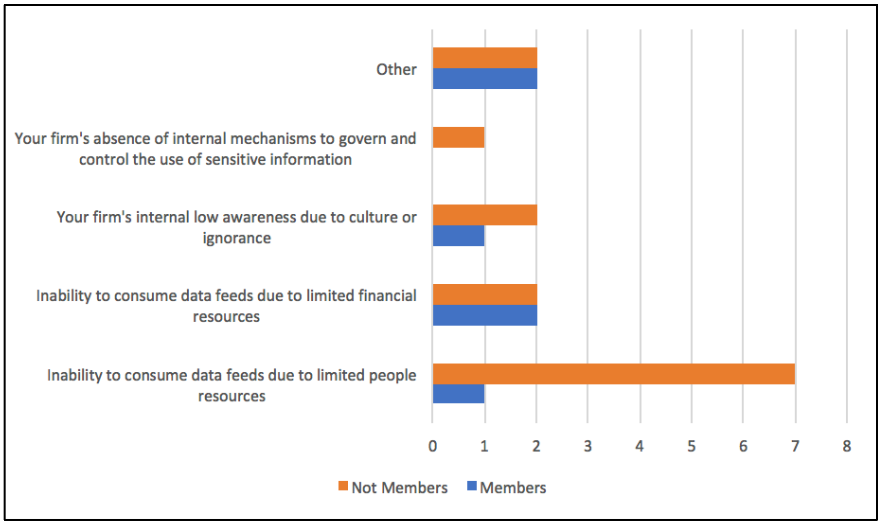

Figure 3 – Organizational Challenges

Incentives of Membership

The next survey question shifted the focus from the barriers impeding membership to the incentives that encourage firms to stay members of information sharing organizations. The question asked:

> When joining a cybersecurity information sharing organization, which membership incentive is the biggest reason for your continued participation?

The survey question provided a selection of the most likely membership incentives derived from the incentive framework described in Part II, plus an 'other' option. The results show that 60% firms join and stay members of sharing organizations primarily to get access to expertise and knowledge disseminated by the organization itself, as well as its other members. For example, 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. This incentive primarily refers to the dissemination of this expertise and knowledge.

In a similar vein, 25% of firms cite getting access to other companies and their threat data as the primary reason they would join or stay members of cyber information sharing organizations. For many sharing organizations, the automated feeds are populated by the information that its members provide, in an anonymized form.

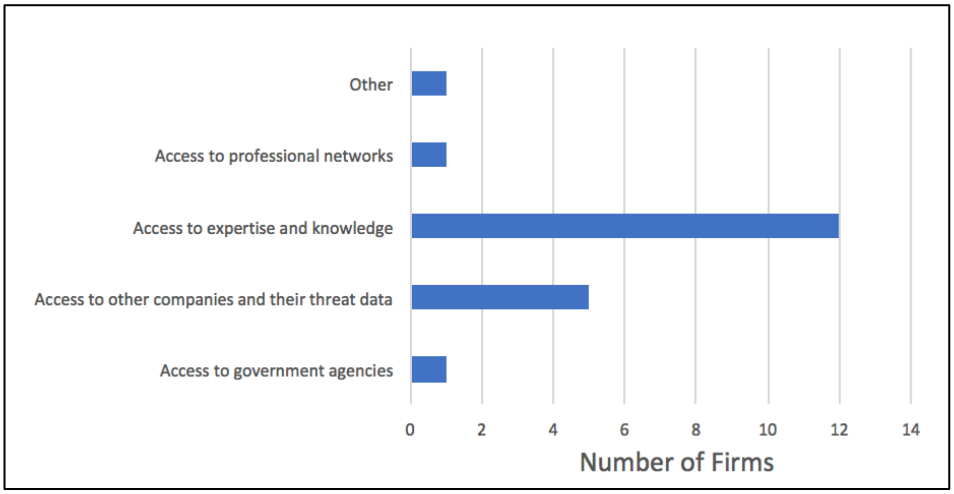

Figure 4 – Membership Incentives

Characteristics of Cyber Information Sharing Organizations

The incentives to join a sharing organization, as well as the barriers that discourage firms to join a sharing organization, are in large part influenced by the characteristics of the sharing organization itself. With the proliferation of cyber information sharing organizations, we now see organizations that come in all shapes and sizes. Some organizations, such as ISACs, are industry focused, while other regional organizations have broader membership profiles. Moreover, some groups are very small, only allowing firms that are competing in a particular product market to join, while others let firms of all sizes with products of all shapes join. However, the effectiveness of each of these organizations varies with the same breadth that can be influenced by a number of factors illustrated in the incentive and barrier framework discussed earlier.

Focusing on the high-level characteristics of cyber information sharing organizations, the survey asked a series of four questions in order to better understand what firms want in a sharing organization. The first question asked:

> Please identify how important it is for your firm to join an organization that has a larger and broader membership profile.

This question originated from the third hypothesis listed above, which says, "Firms are more likely to share information with sharing organizations that have larger memberships."

When examining the results, we see a 70% majority of responses clustered into a region considering a broader membership profile of a sharing organization moderately to very important, with 75% of respondents saying it has above average importance. By examining the results differentiating between members and non-members of sharing organizations, we see that 36% of non-members say a broader membership profile is very important, with 50% saying a larger membership profile of a sharing organization is moderately to very important. On the other hand, 83% of members of sharing organizations say that a broader membership profile is very to extremely important to their continued participation.

Since most respondents that are members of information sharing organizations are from medium to large companies, as discussed above, we can assess that larger firms prefer cyber sharing organizations that have broader membership profiles. In addition, this also supports the hypothesis that firms are more likely to share information with organizations that have larger memberships.

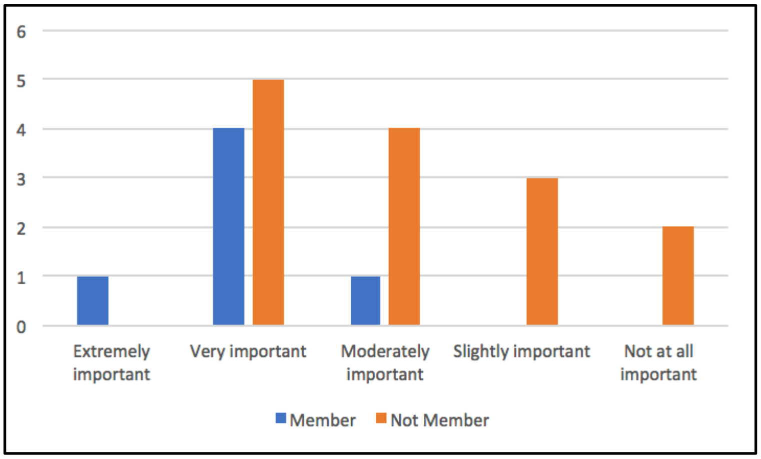

Figure 5 – Importance of Broader Membership Profile

The next question in the series focused on the importance of an organization's industry specialization. The question asked:

> Please identify how important it is for your firm to join an organization that is more specialized to your industry and product market.

The results of this question tell us that a 50% majority view industry specialization of a cyber information sharing organization very to extremely important, with 85% citing this characteristic as having above average importance. Breaking the responses down between members and non-members of sharing organizations, we see from **Figure 6** that 64% of non-members consider industry specialization as very to extremely important, with 93% of non-members saying industry specialization has above average importance.

As compared to the characteristic of a sharing organization having a broader membership profile, non-members, of which a majority are small businesses, view industry specialization of an organization as slightly more important than the size of the group. On the other hand, members of sharing organizations, which are primarily medium to large size companies, view the size of the organization as slightly more important than whether it specializes in a particular industry or product market.

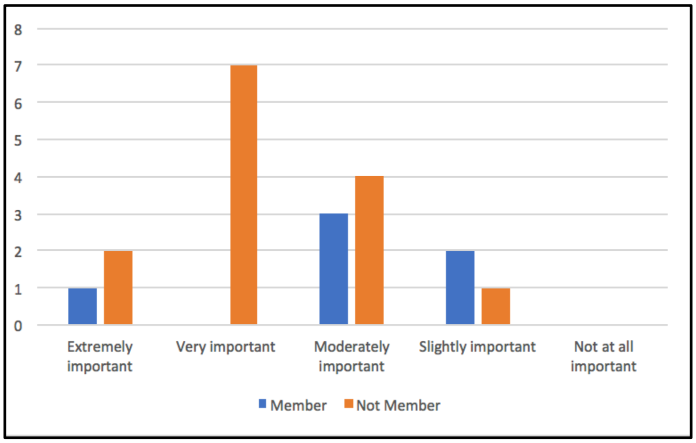

Figure 6 – Importance of Industry Specialization

The third question in the series focused on the importance of an organization having a low cost of membership. The question asked:

> Please identify how important it is for your firm to join an organization that has the lowest cost of membership.

From the results illustrated in **Figure 7**, we see that a 70% majority consider a cyber information sharing organization with a low cost of membership as moderate to very important. However, if we again break down the results between those who are members and non-members of sharing organizations, we see that 79% of non-members view a low cost of membership as moderately to very important, whereas 50% of members view a low cost of membership as not important to slightly important.

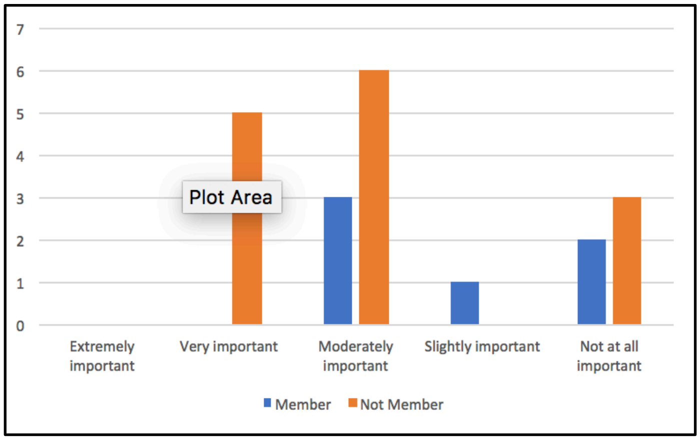

Figure 7 – Importance of Low Cost of Membership

Finally, the fourth question in the series focused on the importance of an organization that does not require a firm to regularly share information in order to be a member. The question asked:

> Please identify how important it is for your firm to join an organization that doesn't require your firm to share information.

With regards to this sharing organization's characteristic, a 45% majority cited it as not important to only slightly important. 35% of the responses considered this characteristic moderately important, whereas a 20% minority cited it as very to extremely important. Differentiating the responses between the members and non-members of a sharing organization, 67% of members viewed this characteristic as moderately important. From this we can assess that the requirement to share information regularly is not a deterrent to their continued membership.

Focusing on the non-members, of those who responded that this characteristic was very to extremely important (23%), all found the cost of membership moderately important. Of those that responded this characteristic is slightly to moderately important (50%), 67% find industry focus very important. Furthermore, of the non-members who cited this characteristic as having above average importance (50%), 85% find the cost of membership moderately important and 71% find industry focus very to extremely important.

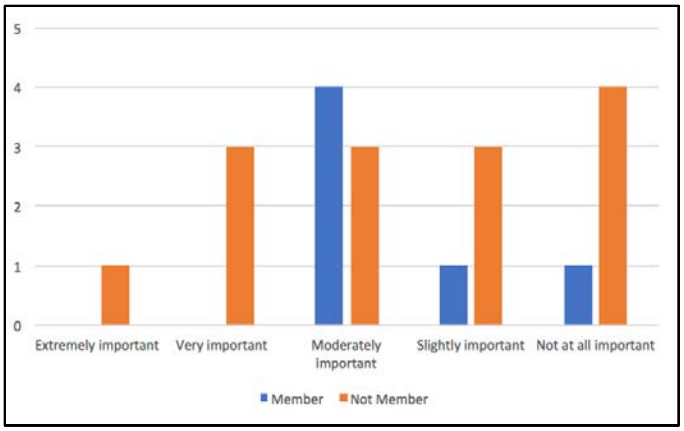

Figure 8 – Importance of Not Requiring Firms to Share Information

Summary of Insights:

Overall, we see that current 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.

Characteristics of the Cybersecurity Information that is Shared

The third section of the survey focused on the types of information that firms share with and receive from the cybersecurity information sharing organizations in which they are members. Understanding the type of information that is actively shared is an important factor in assessing various barriers that firms face internally and externally.

Those who cited that they are members of an information sharing organization were first asked:

What type of information does your firm contribute or share?

An 83% majority responded that they provide content about cyber threats and vulnerabilities to their organizations. These firms also provide information on:

- Incidents (67%)
- Situational awareness (67%)
- Best practices (67%)
- Strategic analysis (50%)

Both members and non-members of cyber sharing organizations were then asked:

What type of information does or would your firm share with other companies / firms?

Other companies or firms in this question refer to companies that are both competitors in the same industry or companies in other industries all together. The responses for this question yielded an interesting difference from the question above. First, an 85% majority of responses said they would be willing to share best practices with other firms. This was followed by 62% saying they would share threats they have identified with other firms, and 54% willing to share mitigators, or pieces of information that lessen the severity or alleviate the impact of cyber-attacks. Other information they would be willing to share include:

- Vulnerabilities (38%)
- Situational awareness (38%)
- Strategic analysis (38%)
- Incidents (31%)

Breaking this down further to focus only on those who are already members of information sharing organizations, we find that members are currently sharing:

- Best Practices (100%)
- Threats (75%)
- Vulnerabilities (50%)
- Mitigators (50%)
- Situational awareness (50%)
- Strategic analysis (50%)

From these two questions, we can assess that firms are more willing to share information about threats and vulnerabilities with cyber information sharing organizations, which often anonymize the data before distributing it to other members, than they are with other firms, whether those are competitors or not. On the other hand, firms are more willing to share best practices with other firms than they are with cyber information sharing organizations.

This last insight could be influenced by the theories of the 'spillover effect,' which normally applied to economic situations tell us that one seemingly unrelated event in one economy can have an impact on other economies. In this case, if firms are directly sharing information with other firms, they are more likely sharing cyber information with firms in their industry or supply chain because those are the companies in which they most likely have regular contact. For this reason, the spillover effect of a certain cyber threat or vulnerability is higher because a cyber-attack on a firm can spread to others it has connections with, similar to financial connections between nations. As a result, sharing best practices are relatively riskless pieces of information to share, as compared to other types of data, because it does not reveal anything about a firm's product, business secrets, or intellectual property that could benefit a competitor, as an example. Best practices can simply describe methods on how to best secure data, protect systems, communicate, train employees, engage with various stakeholders, or how to respond to certain threats, as some examples. Thus, sharing best practices could potentially help minimize damages from the spillover of threats from one firm to another.

Characteristics of the Cybersecurity Information Received

The next set of questions were focused on trying to better understand the utility, quality and timeliness of the information that firms are receiving from cyber information sharing organizations. This part of the survey was derived from the following hypothesis:

- In order for sharing to happen, the information shared must be timely, relevant, and of good utility and quality

Research tells us that if the information is valuable, it is a clear incentive for firms to join an organization and stay a member. When the membership benefits, such as receiving information that assists firms in better protecting themselves from cyber-attacks, no longer exceed the costs, then firms are more likely to end their membership with that organization.

Those who cited they are members were asked the same three questions each with a different qualifying adjective, as shown below:

> How would you best categorize the UTILITY / QUALITY / TIMELINESS of the information you receive from cybersecurity information sharing organizations?

For all three questions, a 50% majority consider the information they receive to be of good utility, quality and timeliness, as illustrated in **Figure 9**. This insight is useful in explaining continued membership in cyber information sharing organizations. If the information these firms are receiving did not provide some utilitarian benefit, then one could surmise that the firm would leave the sharing group. An earlier question revealed that 95% of the firms had not left the sharing organization in which they are members, so this correlates with the insight shown here that they consider the information they receive to be of good quality.

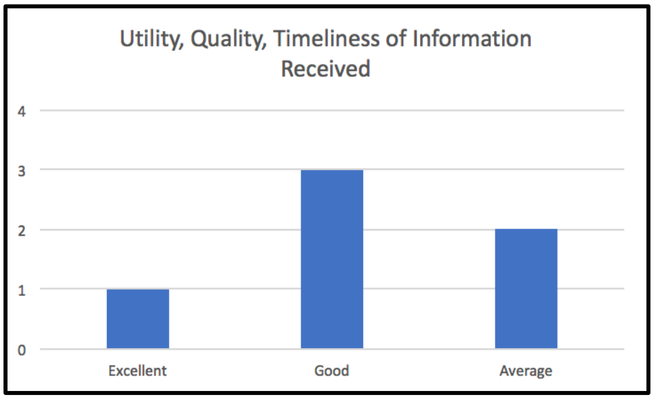

Figure 9 – Utility, Quality, and Timeliness of Information

Impact of Cybersecurity Information on Firm Security Posture

Following insights learned about the utility, quality and timeliness of the information received, firms were next asked about whether this information has helped enhanced its cybersecurity posture. The question asked:

How much does the information you receive from cybersecurity information sharing organization(s) contribute to enhancing your firm's cybersecurity posture?

A 67% majority responded that information they receive has helped enhance their firm's cybersecurity posture 'a lot' to 'a great deal.' The same majority also responded that they 'somewhat agree' to 'strongly agree' that their firm's membership in a cyber information sharing organization has encouraged their firm to make security investments. We can assess from these insights that there is a positive relationship between a firm's membership in a cyber information sharing organization and a firm's cybersecurity posture, which one could use as an important reason for joining a cyber information sharing group.

Which barriers imposing the greatest deterrent to sharing information

The last section of the survey focused on exploring cybersecurity information sharing habits, particularly focusing on identifying which barriers and incentives are the most salient in today's real-world environment. Concentrating on the barriers first, survey participants were asked to rank the eight barriers described in the framework in Section IIII of this paper. Based on previous research as well as interviews, we hypothesized that "Legal barriers are the greatest deterrent to sharing cybersecurity information." In order to assess the validity of this hypothesis, we asked:

Below are characteristics that are often mentioned as barriers to sharing cyber threats and vulnerabilities with cybersecurity information sharing organizations. Please rank them in order of importance for your organization with 1= most important barrier and 8= least important barrier.

Barrier	Description
Constitutional/Legal	Includes privacy concerns as relates to PII/IP, and perceived legal repercussions as relates to disclosure
Technological	Includes lack of interoperability/compatibility between sharing org/firm systems
Informational	Too much information shared and inability to process, applicability of shared information, unreliable data
Collaborative	Includes process complexity, difficulty in establishing trust, lack of reciprocity, type of participants and group size
Managerial	Includes internal risk aversion and mistrust by exposing selves to "uncontrolled risk," poor management of shared information, no agreement establishing trust channels to exchange information
Organizational	Includes inability to consume due to limited resources, absence of mechanisms to govern and control use of information
Performance	Includes reputational damage, loss of customers/revenue from exposure
Cost	Includes high costs of needed system technologies, cost of false positives based on outdated/unreliable data, limited resources to process shared data

This question revealed that a 56% majority think the constitutional / legal barrier is the greatest of the eight shown above, supporting our hypothesis. Indeed, the legal concerns surrounding the sharing of data between businesses as well as with the government is a concern that often gets the most attention in private meetings and conferences alike. Over the last couple years, legislation in Washington, D.C. has only begun to address some of these concerns, assuaging some legality fears, but there is a long way to go in addressing the privacy concerns, risks associated with disclosure and legal liabilities of businesses. Until these issues are addressed, it is likely that information sharing will continue to be a challenge.

Collaborative Barriers

While legal barriers are often mentioned as the most difficult, when discussing information sharing, trust is a topic that also gets raised very frequently. In fact, within the list of hypotheses listed in Section IV, we said:

- No matter the level of risk in a sharing relationship, trust is imperative in order for sharing to occur

Within the barrier framework, establishing trust is categorized as a collaborative barrier, along with process complexity, lack of reciprocity, type of participants, and group size. Since establishing trust is such an important factor in encouraging or deterring the sharing of cybersecurity information, the next question focused on collaborative barriers to gain insights into how firms think about these challenges. The question asked:

In considering collaborative barriers—which include process complexity, difficulty in establishing trust, lack of reciprocity with partners, other members of the sharing organization, and group size—please rank each of these considerations from 1= most important to 5= least important.

The results of the question, shown in **Table 1** below, tell us that the most important collaborative barrier was 'establishing trust,' which supports our hypothesis. The least important collaborative barrier is the size of information sharing group. Interestingly, 'process complexity' did not receive a majority for any ranking, which could be interpreted as meaning this barrier is in fact the least important of the five.

	1	2	3	4	5
Process complexity	13.3%	20%	13.3%	26.7%	26.7%
Establishing Trust	40%	13.3%	26.7%	6.7%	13.3%
Lack of Reciprocity	20%	26.7%	6.7%	40%	6.7%
Type of participants	13.3%	26.7%	40%	6.7%	13.3%
Group Size	13.3%	13.3%	13.3%	20%	40%

Table 1

Maintaining the theme of trying to assess the importance of establishing trust, another question was asked which said:

How important is a legal or informal agreement that establishes trust channels to exchange information between tour firm and the cybersecurity information sharing organization?

Consistent with the findings above, at 67% majority agree that a formal or informal agreement that establishes some level of trust between the firm and cyber information sharing organization is extremely important. In fact, 87% agree that it's very to extremely important. We interpret this insight to mean that 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.

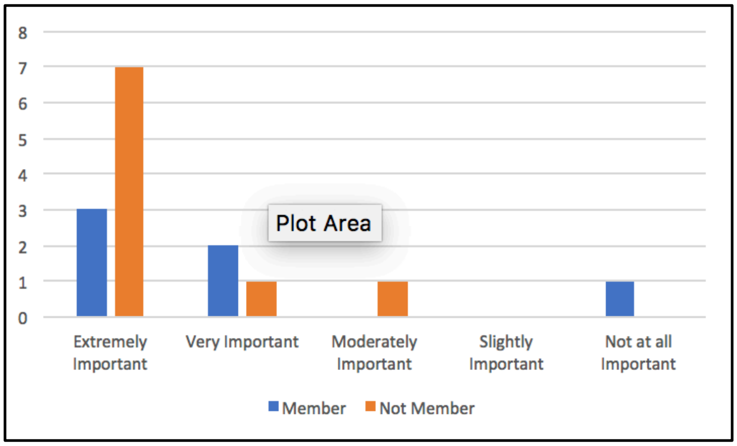

Figure 10 – Importance of Agreements to Establish Trust

While an agreement, whether formal or informal, is one way to incentivize a firm to join a cyber information sharing organization, research has also shown that firms may be more likely to join an organization if they have a trusted relationship with another firm that is already a member. Moreover, since decisions to join an organization are often made by senior management, such as the firm's CISO, if these individuals have a personal, trusted relationship with someone else who is also a member of said sharing organization, they too may be motivated to join. Therefore, along a similar line of questioning, survey participants were asked:

How important was/is having a trusted relationship inside the cyber information sharing organization in motivating you to join the organization?

Again, an 87% majority responded that having a trusted relationship inside the cyber information sharing organization is very to extremely important in motivating them to join the organization themselves.

Which incentives encourage firms to join a cybersecurity organization

After exploring the most salient barriers that deter firms from joining and engaging with cyber information sharing organizations, the survey next explored which incentives were motivating firms the most to join these groups. Based on the literature review and interviews, the following incentives were identified as having the greatest impact:

- Situational awareness
- Legal protections (those already in place)
- Trust and strong partnerships with organization/recipients
- Automation (of sharing of cyber threats and vulnerabilities)
- Reciprocity
- Governance flexibility of sharing organization
- Access that membership provides your firm (i.e. agencies, other companies, expertise, knowledge, expanded professional networks)
- Analysis of vulnerabilities and production capabilities

- Reduced costs/increased productivity
- Improved public image/reputation
- Low-risk organizational network
- Actionable, reliable and relevant information
- Senior management of your firm

Based on these incentives, survey participants were asked to choose from the list above.

What are the top 5 reasons that encouraged you to join and engage with a cybersecurity information sharing organization?

While the results of this question did not conclusively identify any discerning ranking or single incentive as the most important, it did identify 'legal protections' and gaining 'situational awareness' as the two incentives that ranked highest for most important among the options.

REFERENCES

Akbulut, Asli Y. An Investigation of the Factors that Influence Electronic Information Sharing between State and Local Agencies. Louisiana State University, 2002. http://etd.lsu.edu/docs/available/etd-0619103-214616/unrestricted/Akbulut_dis.pdf.

Aviram, Amitai and Tor, Avishalom, Overcoming Impediments to Information Sharing (October 27, 2010). Harvard Law and Economics Discussion Paper No. 427. https://ssrn.com/abstract=435600

Dandurand, L., & Serrano, O.S. (2013). "Towards Improved Cyber Security Information Sharing." *2013 5th International Conference on Cyber Conflict (CYCON 2013), 4-7 June,* 2013.

ENISA (2010). *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*: Available at https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing, Accessed 15th January 2017.

Fernandez Vazquez, D., Pastor Acosta, O., Brown, S., Reid, E., & Spirito, C. (2012). Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships, presented at the 2012 4th International Conference on Cyber Conflict (CyCon 2012): 5-8 June, 2012.

Fransen, Frank, et al. "Cyber Security Information Exchange to Gain Insight into the Effects of Cyber Threats and Incidents." ["Cyber Security-Informationsaustausch zur Erkennung von Cyber-Bedrohungen und -Vorfällen"]. *E & I Elektrotechnik Und Informationstechnik*, vol. 132, no. 2, Mar. 2015, p. 106.

Gal-Or. E., & Ghose, A. (2006). The Economic Incentives for Sharing Security Information. *Information Systems Research*, 16(2), p. 186-208.

Harrison, K., & White, G. (2012). "Information Sharing Requirements and Framework Needed for Community Cyber Incident Detection and Response." *2012 IEEE Conference on Technologies for Homeland Security (HST),* 2012, p. 463.

Headayetullah, Md. and G. K. Pradhan. "Interoperability, Trust Based Information Sharing Protocol and Security: Digital Government Key Issues." 10 Aug. 2010. https://arxiv.org/ftp/arxiv/papers/1008/1008.1670.pdf.

Information Sharing and Analysis Organizations: Putting theory into practice. PwC, April 2016, http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-information-sharing-and-analysis-organizations.pdf

Jackson, Brian A.. How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts. Santa Monica, CA: RAND Corporation, 2014. https://www.rand.org/pubs/research_reports/RR380.html.

National Information Exchange Model (NIEM). Information Sharing Environment, 2013, https://www.ise.gov/mission-partners/national-information-exchange-model-niem.

National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing. The White House, President George W. Bush. October 2007. http://www.nisconsortium.org/portal/resources/bin/National_Strategy_Fo_1423590463.pdf.

Scott E. Jasper (2017) U.S. Cyber Threat Intelligence Sharing Frameworks, International Journal of Intelligence and CounterIntelligence, 30:1, 53-65.

Skopik, F., & Qin Li. "Trustworthy Incident Information Sharing in Social Cyber Defense Alliances." *2013 IEEE Symposium on Computers and Communications (ISCC), 7-10 July,* 2013.

Wagner, Thomas D. Sharing Cyber Intelligence in Trusted Environments – A Literature Review.

Wanying Zhao & White, G. (2012). "Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships." *2012 4Th International Conference on Cyber Conflict (CYCON 2012),* 5-8 June, 2012.

Wilson, T. D. "Information Sharing: An Exploration of the Literature and some Propositions." *Information Research: An International Electronic Journal*, vol. 15, no. 4, 01 Dec. 2010. http://www.informationr.net/ir/15-4/paper440.html.

Zheng, Denise E., & Lewis, James. Cyber Threat Information Sharing: Recommendations for Congress and the Administration. Center for Strategic & International Studies, March 2015, https://pdfs.semanticscholar.org/0208/32b07ce066f4f76a46eac9d7dcc979fb2f89.pdf.

APPENDIX 1: Future Research

Case Studies:

The next step in this research is to put together case studies that can provide some color to the research insights described in this paper. Two possible options have already been started below. While the framework is primarily drawn from the perspective of the firm, an extension of the framework could be applied to the cybersecurity information sharing organization, where one could create a scoring scheme for each incentive and barrier as a way to assess the effectiveness of the sharing organization. The first step in this process has been started below by creating a table to identify which incentives and barriers each sharing organization has.

ISACs: FS-ISAC versus IT-ISAC

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, including the Financial Services ISAC (FS-ISAC) and Information Technology ISAC (IT-ISAC). Despite the model in which they were created, each ISAC operates differently due to differences in size and formality between sectors. They also widely differ in the level of data collection, analysis, and distillation. These differences are briefly discussed below. Using the framework described above

The FS-ISAC was created in 1999 in response to PDD-63. Today, the FS-ISAC is considered the most formalized ISAC, working with firms in the financial services space, as well as commercial security firms. In 2013, the FS-ISAC extended its services to share information with financial services firms worldwide, including information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources. Due to the importance of the global financial services infrastructure and the resilience of individual firms against cyber attacks that could significantly impact the entire sector's ability to provide critical services that impact the global economy, the FS-ISAC has only grown in importance over the past 17 years. Today, the FS-ISAC has 1000s of members, whose names are not made public.

The IT-ISAC was founded in 2002 by 19 prominent IT industry companies, including Microsoft, IBM, Oracle, and Computer Sciences. The IT-ISAC is modeled after the financial services group, which distributes much of its information anonymously. Moreover, when the IT-ISAC was stood up, there was a gap in the ecosystem in how large IT vendors communicated risks and vulnerabilities with customers, designating a clear need for the creation of the IT-ISAC. Since then, most of its founding members have grown and matured their own processes for communicating directly with customers, so over time, the IT-ISAC wasn't offering as much value for large-scale customers. As a result, the IT-ISAC decided to shift its focus in order to retain importance. Rather than serving as a sharing organization for primarily IT companies, it decided to try and serve a broader market, which is reflected by the various interest groups that member companies can participate, particularly the food and agriculture interest group. Today, the IT-ISAC has 42 members, which are listed on its website.

Recognizing the significant differences between the FS-ISAC and IT-ISAC, we can apply the framework for information sharing incentives and barriers described in sections II and III to attempt to better understand why one is more effective than the other.

INCENTIVE	FS-ISAC	IT-ISAC
Situational Awareness	Disseminates automated threat feeds, provides security best practices, trainings, workshops, webinars, special events to provide members with better cyber situational awareness	Releases daily threat reports, alerts, shares threats via an automated sharing platform, convenes subject or industry-specific special interest groups, and has a technical committee for members to gain access to security analysts, experts and executives
Legal		
Technological	Uses automation to send and receive information about threats and vulnerabilities. Information is distributed anonymously	Uses a threat intelligence platform that stores, aggregates, and contextualizes thousands of indicators using the STIXX/TAXI framework for automated sharing
Costs		Two lower-tired membership levels are affordable for small to medium-sized businesses
Management		
Informational	Information is both collected and disseminated.	Information is both collected and disseminated.
Performance		
Collaborative	Network is collaborative and builds trust with members, so that members continue to participate	Network is collaborative and aimed at bringing companies together to minimize threats

BARRIER	FS-ISAC	IT-ISAC
Constitutional / Legal	Privacy concerns still arise due to select instances of disclosure of personal information following an attack	
Technological		
Informational	Members often say too much information is shared and they cannot process/analyze everything	Concerns with applicability and quality of information shared
Collaborative	Free-riders are a problem, as not all membership levels require firms to contribute. Some members get access others do not due to special status and exclusive groups. Members are firms of all sizes, with varying level of capabilities. Many members are competitors	
Managerial		
Organizational		
Performance		
Cost	Cost of membership can be expensive to some firms, and access/participation in initiatives depends on membership level	Cost of membership can be expensive to some firms, and access/participation in initiatives depends on membership level

APPENDIX 2: Survey

Incentives and Barriers to Sharing

A. Thank you for assisting with our research on cybersecurity information sharing incentives and barriers. We are interested in your organization's practices and interactions with organizations that share cybersecurity information. Our focus is on the characteristics that incentivize your firm to share and the barriers that discourage sharing. This survey should take no more than 20 minutes of your time to complete. Please answer every question and hit submit at the end. Your responses are completely confidential, unless you chose to provide your contact information at the end. In exchange for your time, we are happy to share the results of the survey, as well as the final report. If you have any questions or comments, please email pkoepke@mit.edu. Thank you for your help and valuable time!

Q1 Please identify your industry or sector

- ☐ Banking and Financial Services
- ☐ Government - State/Local
- ☐ Government - National/International
- ☐ Professional Services
- ☐ Insurance
- ☐ Retail and Wholesale
- ☐ Software Publishing and Internet Services
- ☐ Education
- ☐ Construction, Materials and Natural Resources
- ☐ Industrial Manufacturing
- ☐ Transportation
- ☐ Energy
- ☐ Pharmaceuticals, Life Sciences and Medical Products
- ☐ Telecommunications
- ☐ Travel and Hospitality
- ☐ Food and Beverage Processing
- ☐ Healthcare Providers
- ☐ Media and Entertainment
- ☐ Industrial Electronics and Electrical Equipment
- ☐ Chemicals
- ☐ Other

Q2 Number of employees in your organization:

○ Fewer than 1,000

○ 1,000 to 9,999

○ 10,000 or more

B. Cyber Information Sharing Organizations: For the next section, we are interested in your relationships with the organizations with which you share cybersecurity information. These can include organizations such as ISACs, CERTs and the Cyber Threat Alliance, or other similar information sharing organizations. Note: From this point forward, "you" is referring to the organization that you represent.

Q4 Is your firm a member of any cybersecurity information sharing organization(s)?

○ Yes

○ No

Q6 Please list which organization(s):

Q7 How often do you engage with the cybersecurity information sharing organization(s) you listed above? Engagement could include participation in meetings, webinars, conference calls, etc. If you listed multiple organizations, please chose the frequency with the one organization that you engage the MOST.

○ Daily

○ 1-3 times a week

○ 1-4 times a month

○ Once every quarter

○ 1-3 times a year

○ Never

○ N/A

Q8 If you listed multiple organizations, please circle the frequency that describes your engagement with the organization with which you share information or engage with the LEAST.

○ Daily

○ 1-3 times a week

○ 1-4 times a month

○ Once every quarter

○ 1-3 times a year

○ N/A

Q9 Do you pay for membership in any of the cybersecurity information sharing organizations you listed above?

○ Yes

○ No

Q10 Is your firm in a leadership role(s) in any of the organizations you listed above?

○ Yes

○ No

Q11 How long has your firm been a member of the cybersecurity information sharing organization(s) you listed above? If you listed more than one organization, please focus on the one with which you have had the longest relationship.

○ Less than 3 months

○ 3 months to 1 year

○ Between 1 -5 years

○ More than 5 years

○ N/A

Q12 Has your firm left a cybersecurity information sharing organization at any point within the last 5 years?

○ Yes

○ No

Q13 Why have you not joined other / any cybersecurity information sharing organization(s)?

○ Cost of membership

○ Lack of information quality, utility, value

○ Inability to manage additional information processing

○ Other ____________________

Q14 What was the primary reason that your firm decided to leave this organization?

○ Membership cost was not in my budget

○ Information I received was not valuable

○ Joined a different organization

○ Other ____________________

Q15 Which organizational challenges most impacted or would impact your firm’s decisions to not join or terminate a membership in a cybersecurity information sharing organization?

❍ Inability to consume data feeds due to limited people resources

❍ Inability to consume data feeds due to limited financial resources

❍ Inability to consume data feeds due to technological resources

❍ Your firm's internal low awareness due to culture or ignorance

❍ Your firm's absence of internal mechanisms to govern and control use of sensitive information

❍ Other ____________________

Q16 When joining a cybersecurity information sharing organization, which membership incentive is the biggest reason for your continued participation?

❍ Access to government agencies

❍ Access to other companies and their threat data

❍ Access to expertise and knowledge

❍ Access to professional networks

❍ The safe harbor aspect of membership, including motivation by audits

❍ Other ____________________

Q17 Please identify how important it is for your firm to join an organization that has a large and broader membership profile

❍ Extremely important

❍ Very important

❍ Moderately important

❍ Slightly important

❍ Not at all important

Q18 Please identify how important it is for your firm to join an organization that is more specialized to your industry and product market

❍ Extremely important

❍ Very important

❍ Moderately important

❍ Slightly important

❍ Not at all important

Q19 Please identify how important it is for your firm to join an organization that has the lowest cost of membership

○ Extremely important
○ Very important
○ Moderately important
○ Slightly important
○ Not at all important

Q20 Please identify how important it is for your firm to join an organization that doesn't require your firm to share information

○ Extremely important
○ Very important
○ Moderately important
○ Slightly important
○ Not at all important

C. Cybersecurity Information You Share: In this section, we are interested in the information you contribute or share with cybersecurity information sharing organizations and other firms.

Q21 Does your firm contribute by providing content, i.e. information about cyber vulnerabilities or threats, to any cybersecurity information sharing organization?

○ Yes
○ No

Q22 What type of information does your firm contribute or share? Please select all that apply.

□ Incidents
□ Threats
□ Vulnerabilities
□ Mitigators
□ Situational Awareness
□ Best Practices
□ Strategic Analysis
□ Other ____________________

Q23 Which type of other company/firm (not cybersecurity information organization) are you more likely to share your firm's cybersecurity information? Please select all that apply.

□ Same relative size
□ Same industry
□ Smaller size
□ Different industry
□ Larger size
□ I don't/won't share with other companies

Q24 What type of information does or would your firm share with other companies/firms? Please select all that apply.

□ Incidents
□ Threats
□ Vulnerabilities
□ Mitigators
□ Situational Awareness
□ Best Practices
□ Strategic Analysis
□ Other ____________________

D. Cybersecurity Information You Receive: We would now like to understand the value of the information you receive from cybersecurity information sharing organizations.

Q25 How would you best categorize the UTILITY of the information you receive from cybersecurity information sharing organizations?

○ Excellent
○ Good
○ Average
○ Poor
○ Terrible

Q26 How would you best categorize the QUALITY of the information you receive from cybersecurity information sharing organizations?

○ Excellent
○ Good
○ Average
○ Poor
○ Terrible

Q27 How would you best categorize the TIMELINESS of the information you receive from cybersecurity information sharing organizations?

- ○ Excellent
- ○ Good
- ○ Average
- ○ Poor
- ○ Terrible

Q28 How much does the information you receive from cybersecurity information sharing organization(s) contribute to enhancing your firm's cybersecurity posture?

- ○ A great deal
- ○ A lot
- ○ A moderate amount
- ○ A little
- ○ None at all

E. Cybersecurity Information Sharing Habits: We would now like to know about your information sharing behaviors and perceived barriers to sharing.

Q29 Your firm's involvement in cyber information sharing organizations has encouraged your firm to make security investments because of the important or revealing information it has received by being a member?

- ○ Strongly agree
- ○ Somewhat agree
- ○ Neither agree nor disagree
- ○ Somewhat disagree
- ○ Strongly disagree

Q30 Below are characteristics that are often mentioned as barriers to sharing cyber threats and vulnerabilities with cybersecurity information sharing organizations. Please rank them in order of importance for your organization with 1= most important barrier and 8= least important barrier. *Please use each number only once for the blanks below.

Barrier	Description
Constitutional/Legal	Includes privacy concerns as relates to PII/IP, and perceived legal repercussions as relates to disclosure
Technological	Includes lack of interoperability/compatibility between sharing org/firm systems
Informational	Too much information shared and inability to process, applicability of shared information, unreliable data
Collaborative	Includes process complexity, difficulty in establishing trust, lack of reciprocity, type of participants and group size
Managerial	Includes internal risk aversion and mistrust by exposing selves to "uncontrolled risk," poor management of shared information, no agreement establishing trust channels to exchange information
Organizational	Includes inability to consume due to limited resources, absence of mechanisms to govern and control use of information
Performance	Includes reputational damage, loss of customers/revenue from exposure
Cost	Includes high costs of needed system technologies, cost of false positives based on outdated/unreliable data, limited resources to process shared data

______ Constitutional / Legal
______ Technological
______ Informational
______ Collaborative
______ Managerial
______ Organizational
______ Performance
______ Cost

Q31 In considering collaborative barriers -- which include process complexity, difficulty in establishing trust, lack of reciprocity with partners, other members of the sharing organization, and group size -- please rank each of these considerations from 1= most important to 5= least important. *Please only use 1-5 once for each of the blanks below
______ Process complexity
______ Establishing trust
______ Lack of reciprocity
______ Type of participants
______ Group size

Q32 How important is technological compatibility/ interoperability for how information is shared between the cybersecurity information sharing organization and your firm?

○ Extremely important
○ Very important
○ Moderately important
○ Slightly important
○ Not at all important

Q33 How important is a legal or informal agreement that establishes trust channels to exchange information between your firm and the cybersecurity information sharing organization?

○ Extremely important
○ Very important
○ Moderately important
○ Slightly important
○ Not at all important

Q34 In a trusted environment -- meaning an environment in which you are comfortable sharing cyber information in a mutually beneficial way due to a formalized agreement, personal relationship, or security-clearance -- what level of risk versus benefits for your firm are you willing to accept to share and receive information? Select all that apply.

□ Low risk, low benefit
□ Low risk, high benefit
□ High risk, low benefit
□ High risk, high benefit

Q35 Many cybersecurity information sharing organizations have automated processes to send and share cyber threat information with members and partners. How important are these organization's automation capabilities for your firm?

○ Extremely important
○ Very important
○ Moderately important
○ Slightly important
○ Not at all important

Q36 Which reasons contributed to that importance?

□ Anonymizes identity of submitter

□ Minimizes amount of data collected

□ Retains information for a limited period of time

□ Ensures information used for authorized government purposes

□ Sharing language that is simple and efficient, uniform and clear

□ Other ____________________

Q37 Please tell us which of these characteristics would increase the importance of an organization's automated delivery of cyber threat information?

○ Anonymizes identity of submitter

○ Minimizes amount of data collected

○ Retains information for a limited period of time

○ Ensures information used for authorized government purposes

○ Sharing language that is simple and efficient, uniform and clear

○ Other ____________________

Q38 What are the top 5 reasons -- from the list provided below -- that encouraged you join and engage with a cybersecurity information sharing organization? Please choose the top 5 reasons for your firm from the list on the left and rank them by dragging each into its corresponding box, with 1= the most important incentive and 5= the least important incentive.

1	2	3	4	5
_______ Situational Awareness _______ Legal Protections (those already in place) _______ Trust and strong partnerships with organization/ recipients _______ Automation (of sharing of cyber threats and vulnerabilities _______ Reciprocity	_______ Situational Awareness _______ Legal Protections (those already in place) _______ Trust and strong partnerships with organization/ recipients _______ Automation (of sharing of cyber threats and vulnerabilities _______ Reciprocity	_______ Situational Awareness _______ Legal Protections (those already in place) _______ Trust and strong partnerships with organization/ recipients _______ Automation (of sharing of cyber threats and vulnerabilities _______ Reciprocity	_______ Situational Awareness _______ Legal Protections (those already in place) _______ Trust and strong partnerships with organization/ recipients _______ Automation (of sharing of cyber threats and vulnerabilities _______ Reciprocity	_______ Situational Awareness _______ Legal Protections (those already in place) _______ Trust and strong partnerships with organization/ recipients _______ Automation (of sharing of cyber threats and vulnerabilities _______ Reciprocity

_______ Governance flexibility of sharing organization _______ Access that membership provides your firm (i.e. agencies, other companies, expertise, knowledge, expanded professional networks) _______ Analysis of vulnerabilities and production capabilities _______ Reduced costs/ increased productivity _______ Improved public image/ reputation _______ Low-risk organizational network _______ Actionable, reliable and relevant information _______ Senior management of your firm	_______ Governance flexibility of sharing organization _______ Access that membership provides your firm (i.e. agencies, other companies, expertise, knowledge, expanded professional networks) _______ Analysis of vulnerabilities and production capabilities _______ Reduced costs/ increased productivity _______ Improved public image/ reputation _______ Low-risk organizational network _______ Actionable, reliable and relevant information _______ Senior management of your firm	_______ Governance flexibility of sharing organization _______ Access that membership provides your firm (i.e. agencies, other companies, expertise, knowledge, expanded professional networks) _______ Analysis of vulnerabilities and production capabilities _______ Reduced costs/ increased productivity _______ Improved public image/ reputation _______ Low-risk organizational network _______ Actionable, reliable and relevant information _______ Senior management of your firm	_______ Governance flexibility of sharing organization _______ Access that membership provides your firm (i.e. agencies, other companies, expertise, knowledge, expanded professional networks) _______ Analysis of vulnerabilities and production capabilities _______ Reduced costs/ increased productivity _______ Improved public image/ reputation _______ Low-risk organizational network _______ Actionable, reliable and relevant information _______ Senior management of your firm	_______ Governance flexibility of sharing organization _______ Access that membership provides your firm (i.e. agencies, other companies, expertise, knowledge, expanded professional networks) _______ Analysis of vulnerabilities and production capabilities _______ Reduced costs/ increased productivity _______ Improved public image/ reputation _______ Low-risk organizational network _______ Actionable, reliable and relevant information _______ Senior management of your firm

Q39 How important was/is having a trusted relationship inside the cyber information sharing organization in motivating you to join the organization?

❍ Extremely important
❍ Very important
❍ Moderately important
❍ Slightly important
❍ Not at all important

Q40 How much does a competitor's participation in a cybersecurity information sharing organization incentivize your firm to also participate?

❍ A great deal
❍ A lot
❍ A moderate amount
❍ A little
❍ None at all

Q41 How much has your membership in and engagement with a cybersecurity information sharing organization increased your firm's remediation abilities following an attack?

❍ A great deal
❍ A lot
❍ A moderate amount
❍ A little
❍ None at all

Q42 Willingness to be contacted in the future: Would you be willing to share your contact information with us, only for the purposes of any follow up questions or clarification, and with continuing confidentiality?

❍ Yes
❍ No

Q43 Thank you. Please provide your name, organization, and email below.