2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships

Diego Fernández Vázquez,
Oscar Pastor Acosta
Defence and Security Division
ISDEFE
Madrid, Spain
{dfvazquez, opastor}@isdefe.es

Sarah Brown,
Emily Reid
Cyber Security Division
The MITRE Corporation
Bedford, MA 01730
{sbrown, ereid}@mitre.org

Christopher Spirito
International Operations
The MITRE Corporation
Bedford, MA 01730
cspirito@mitre.org

Abstract: Information and Communication Technologies are increasingly intertwined across the economies and societies of developed countries. Protecting these technologies from cyber-threats requires collaborative relationships for exchanging cyber defense data and an ability to establish trusted relationships. The fact that Communication and Information Systems (CIS) security[1] is an international issue increases the complexity of these relationships. Cyber defense collaboration presents specific challenges since most entities would like to share cyber-related data but lack a successful model to do so.

We will explore four aspects of cyber defense collaboration to identify approaches for improving cyber defense information sharing. First, incentives and barriers for information sharing, which includes the type of information that may be of interest to share and the motivations that cause social networks to be used or stagnate. Second, collaborative risk management and information value perception. This includes risk management approaches that have built-in mechanisms for sharing and receiving information, increasing transparency, and improving entity peering relationships. Third, we explore procedural models for improving data exchange, with a focus on inter-governmental collaborative challenges. Fourth, we explore automation of sharing mechanisms for commonly shared cyber defense data (e.g., vulnerabilities, threat actors, black/white lists).

In order to reach a common understanding of terminology in this paper, we leverage the NATO CIS Security Capability Breakdown [19], published in November 2011, which is designed to

1 The ability to adequately protect the confidentiality, integrity, and availability of Communication and Information Systems (CIS) and the information processed, stored or transmitted.

identify and describe (CIS) security and cyber defense terminology and definitions to facilitate NATO, national, and multi-national discussion, coordination, and capability development.

Keywords: *information sharing, cyber defense, framework*

1. INTRODUCTION

Information and Communication Technologies are increasingly intertwined across the economies and societies of developed countries. Protecting these technologies from cyber-threats[2] requires collaborative relationships for exchanging cyber defense[3] information and an ability to establish trusted relationships. The fact that cyber defense is an international issue increases the complexity of these relationships. Cyber defense collaboration presents specific challenges since most entities would like to share cyber defense data but lack a successful model to do so that takes into account the cultural perspectives of sharing and information exchange. We will explore the following four aspects of cyber defense collaboration to identify approaches for improving cyber defense information sharing:

- **Incentives and barriers for information sharing.**
  Aimed to identify the static structure of the information sharing network, and mainly trying to find answers of Why, Who and What of the network.
- **Information value perception and collaborative risk management.**
  Entities share information according to its perceived value, purpose, and meaning; thus, it is critical to ensure all entities have a common understanding of the information to be shared. It is critical to ensure all entities have a common understanding of the information to be shared. Depending on the nature and scope of the network, the approaches for collaborative risk management have to be shaped according to the prevention or response approach of the collaboration.
- **Improving data exchange.**
  Many cyber defense sharing networks suffer from an over-generalised concept of operations. Procedural models provide a structure that defines how information will flow across operational components. These models must address the information needs of the individual participants within each nation in order to provide sought-after information in a clear way. Bringing together information from complementary angles helps participants to derive results for problems that they cannot address individually.
- **Automation of sharing mechanisms for technical cyber defense data.**

A cyber defense information-sharing network is likely to contain a huge amount of technical data. Automation on the selection of that data and the mechanisms to share with participants

2 Threats are threat sources (or agents) with capability and intent, modeled as generic threats and specific threats. For example, Internet threats could be an instance of a generic threat and a certain hacker group could be an instance of a specific threat. Threat capability includes the ability of a threat source to perform certain activities such as using, customizing, and creating exploits, performing cryptanalysis, social engineering, etc. This can also include the various tools and resources that are available to the threat. This information can be tied to the CIS information for risk assessment. [12]

3 The ability to safeguard the delivery and management of services in an operational Communications and Information Systems (CIS) in response to potential and imminent as well as actual malicious actions that originate in cyberspace. [12]

in the framework of a specific network is a key requirement to facilitate effective analysis and sharing. Moreover, the existence of an automated exchange can provide an incentive for joining the trusted network; automation increases the benefit the parties involved by receiving data quickly and eases the process of contributing data to the network.

2. INCENTIVES AND BARRIERS FOR INFORMATION SHARING

There is a long history across the cyber defense community of establishing information sharing repositories, creating data-exchange standards, and finding the repositories underutilised.

There is a significant amount of research on approaches for information sharing. However, within the field of cyber defense, there is debate about:

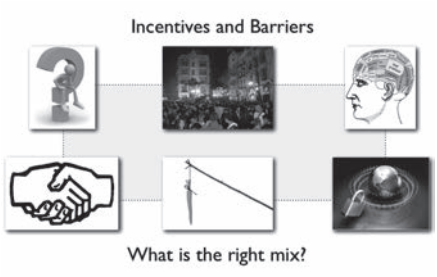
- Data types that are useful to share.
- Organizational and national policies about what can be shared.
- Models for sharing.
- How best to address privacy and security.

These questions, in which answers are still developing for the cyber defense community, add an additional challenge for sharing, because cyber defense is still not a well-defined, stable field. In addition to the maturity needed to determine what data to share and how to share it securely, more research is needed to understand social aspects of sharing. Engineers focus on technical aspects of information sharing networks, and often do not take into consideration the social, organizational, and cultural systems of use. In short, the motivations that cause communities to not engage in sharing or let a sharing relationship stagnate are not well understood. [10]

The European Network and Information Security Agency (ENISA) recently published a report on the barriers to and incentives for information sharing in the field of network and information security[1]. Taking these findings into account and to further our understanding of the motivations behind joining and participating in an information sharing community, we will explore the following:

- Why is the information-sharing network needed?
- Who will participate?
- What information is desired? What information will be shared/restricted?
- Does the network require services for confidentiality, integrity, privileged access and anonymity?
- What are the principles, challenges, and benefits in a cyber defense information-sharing network that will entice the right audience and achieve target objectives?
- Understanding incentives within information sharing networks
- Establishing, Perceiving and Maintaining Trust

FIGURE 1. I INCENTIVES AND BARRIERS INFOGRAPHIC



Why is the information-sharing network needed?
The network needs common scope and shared targets with the participants to reach the expected objectives of the information sharing from every participant. The scope specifies the approach – prevention, response or both - of the network.

Who will participate?
Once the scope and the objectives of the network are defined, the characterisation of the expected participant would be required based on organisational and individual aspects, for instance: the entity nature (public or private), network membership (mission or permanent), the scope of the organisation (national or supranational), and the functional role (technician or decision maker / governance). This information will allow for the creation of sharing profiles, used by sharing network participants to facilitate information exchange.

What information is desired? What information will be shared/restricted?
In addition to technical data, best practices and risk assessments may be of interest to share, attending to the role of the participants.

Does the network require services for confidentiality, integrity, privileged access, and anonymity?
The relationships between the participants need to be defined according to the requirements of the information to share. The specification of different scenarios will be necessary to consider the various options that may occur in the exchange of information to build trust between the players, either by the quality of information exchanged, authentication of its source, ensure the delivery of the information to authorised recipients or guarantee the anonymity of authorised participants.

What are the principles, challenges, and benefits in a cyber defense information-sharing network that will entice the right audience and achieve target objectives?
Entities participate in sharing networks when their return is more than the cost to participate. The identification of the benefits - for instance: cost savings, quality of information or network's relevance to the organisation - and the challenges - for instance: achievement of a high quality of information or establishment of clear and agreed management rules - of every potential participant will help to build the collaboration network and the principles that it is based on.

Understanding incentives within information sharing networks
The procedural model and its components must identify and use the incentives for sharing between participating entities. An assessment must be made of each participating entity type, their ability to produce products with perceived value, and the underlying incentives, such that the incentives can be threaded into the established sharing network procedures. Information economy aspects could be structured in financial incentive models that should be integrated into procedural models.

Establishing, Perceiving and Maintaining Trust
In an ENISA study of successful public private partnerships [6], one recommendation is about the importance of Trust Building Policies. The ENISA study reports that in information sharing networks where information sharing is the core service provided, a key requirement is a high degree of trust in the network itself (i.e., that the policies, membership rules, requirement for security clearance, and interaction type must have been carefully designed to support trust.

Trust between entities need not be whole or persistent. Transient trust during a moment of crisis may allow for a piece of information to be shared between two entities that would have not otherwise been made available for consumption. A sliding trust scale that is influenced by other factors such as operational need and quality of relationship must be incorporated into a sharing network to accommodate information sharing relationships that change in form over time. The partner you don't trust today may be your best friend tomorrow.

Trust relationships must span the different engagement levels: from the organisational leaders that empower their staff to produce and consume information to the technical staff that ultimately will take the information and put it to use. Having an institutional process for guiding these types of relationships is central to the success of an organisation as a whole in participating in information sharing networks. To support these processes organisations will need to focus on the trust scale while leveraging mechanisms and tools to support the mapping and perception of these relationships.

Trust relationships are affected by both the organizational and ethnic cultures of the sharing entities. There are cultures where no information sharing will take place until a maturity point is reached in the relationship. Then there are ethnic cultures where a business need will drive information sharing even though the relationship has not matured enough for sustained information sharing between entities.

3. INFORMATION VALUE PERCEPTION AND COLLABORATIVE RISK MANAGEMENT

Entities share information according to its perceived value, purpose, and meaning; thus, it is critical to ensure all entities have a common understanding of the information to be shared. At the human and machine level, establishing trust and effective communication requires a common vocabulary and taxonomy, especially between nations with different languages. For example, in this paper, we refer to the NATO CIS Security Capability Breakdown [12] to ensure

a common understanding of CIS and cyber defense terminology that appears. The CIS security capability breakdown is designed to specifically facilitate NATO, national, and multi-national discussion, coordination, and capability development related to CIS security and cyber defense.

When we look further into how entities view of particular piece of data or situation, we find this topic explored by "ethnomethodologists", who use the phrase "sense-making" to refer to observable behaviours in which individuals orient toward the same aspect of the world and demonstrate to each other – through detailed enactment of practices – that they share that orientation. "Mutual orientation toward an object" includes:

- Perception (we're looking at the same thing),
- Interpretation or instructed perception (we're looking at the same aspects of, or applying the same framework on, that thing), and
- Conventions or instructed actions (we display similar behaviours with respect to use of that thing; the modifier "instructed" refers to the fact that we learn those behaviours from on another, primarily by example)." [2]

This first step in the analysis of an information sharing relationship is critical, especially when two or more countries and cultures are involved. There must be an agreement from all parties that the shared perception of the objects in the repository exists. The second step is to ensure that all parties agree upon the analysed characteristics of the framework. Lastly, there needs to be an ability to include the behavioural components of information sharing so that acceptable boundaries are placed around. Standards ensure entities agree on the information to share and can exchange it.

Assessing and mitigating existing risks is easier than anticipating unknown risks. Thus, risk management approaches should include collaborative models with built-in mechanisms for sharing and receiving information, increasing transparency, and improving entity peering relationships. These approaches should facilitate government relationships and public-private partnerships.

Traditional risk management usually consist of two phases, no matter what is the applied methodology such as NIST SP800-30 [3], ISO 27005 [4], or MAGERIT [5], aimed to gather the risk awareness in a specific time that has to be updated– usually yearly - in a regular basis:

- risk assessment that could be generally described as an identification of assets, threats and countermeasures to obtain assessments of the risk stemming from the impact on the assets
- risk management where it takes into account the risk assessment to make decisions on how every identified risk will be managed.

In case that the information sharing network is focused on the prevention approach, the information flow should be related to preparation against threats that can exploit vulnerabilities causing impacts on assets. Sharing of new or evolved vulnerabilities, patterns of threats, new or evolved threats, technical countermeasures and non-technical countermeasures are expected.

In case that the information sharing network is focused on the response approach, the information flow should be related to how the risk is managed mainly in the response to and recovery from the attacks based on the impact. Sharing of how the collaboration could be more efficient, how mutual aid agreements could be adopted, identification of cascading effects, practices to improve the efficiency on the recovery of services, operational responses to attacks and collaboration procedures are expected.

But there will be a subjective factor on the risk management because of the diverse rules or perception on definitions of threat levels, identification of relevant assets, identification of countermeasures to apply and how the impact is considered as relevant in organisations. Organisations could come from diverse cultures/sectors (the principal assets to protect) and countries (diverse languages could cause difficulties since translated words and sentences may not have the exact or equivalent meaning) that could produce some misunderstandings on how the risk is managed within an environment of aggregated risk management where cascading effects have to be avoided and the trust among participants of the sharing network needs to be held or improved to foster their collaboration.

As the situational awareness of the cyberspace related to an organisation is in a very changing environment, a specific organisation can take data related to the status of cyber defense in order to calculate in real time the threat level and share with participants of its collaboration network. An agreement on how the threat level is calculated and the meaning of each threat level – in terms of expected impact and expected actions of reaction - is envisaged as a mandatory pre-requirement for collaborations based on mutual understanding of the different risk management approaches. This could support a dynamic risk management where threat levels are calculated in real time, as opposite to traditional risk management, and providing the appropriated information to decision makers about how the risk have to be deal with – updating the threat awareness support a quick, efficient and adaptable reaction to the changing attack environment - and how to anticipate risk to selected participants – for instance based on mutual aid collaboration agreements - of the collaboration network.

4. PROCEDURAL MODEL FOR IMPROVING DATA EXCHANGE

Many cyber defense sharing networks suffer from an over-generalised concept of operations. Procedural models[4] must dictate how information will flow across operational components so that flows can be optimised and information products can be integrated into decision trees.

Information exchange models must address the information needs of the individual participants within each nation in order to provide sought-after information in a clear way. The data sharing network should bring together information from complementary angles, allowing participants to derive results for problems that are difficult to address individually. Aspects that must be considered to design effective procedural models for a cyber defense sharing network include:

4 The generally simplified representation of an aspect of reality expressed in a specified manner so as to facilitate reasoning about that aspect.[12]

- Participant Roles
- Governance Structure
- Institutional Funding
- Enabling Collaboration
- Information Protection and Release Control
- Incorporating Financial Incentive Models

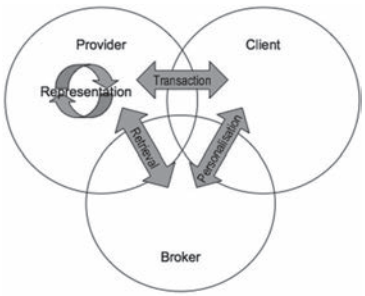
Participant Roles

We know from experience that the value of information varies based upon the needs of the consumer. Each information consumer assigns values to the types of information they need in the moment. Each information producer assigns a value or cost for the piece of information they are sharing. A successful information sharing network will bring together information producers and consumers with minimal friction. To achieve this, each participant must be assigned a role for a specific transaction. Participants may act in various roles within the information sharing network, but for any transactions, we must be able to define the role held by each participant in that transaction.

When we talk about participants, we are not limited to participants as individuals. Rather we are taking the view that a participant can be a non-organisationally associated individual on one end of the spectrum, or a multinational entity that has multiple types of participants within it at the other end of the spectrum. We do exclude non-human participants such as Artificial Intelligence backed systems.

Roland Klemke in his Modeling Context in Information Brokering Processes thesis states that "three different roles participate in the information brokering process: the provider who offers information, the consumer who demands information, and the broker who mediates between the other two. Different roles in this view not necessarily have to be represented by different persons, a role may even be represented by fully automated processes." [16] We also include the role of Information Producer as we recognise in the world of cyber security the producer of information may often not be the provider offering the information to a community.

FIGURE 2. THE SEMANTIC WEB WITH INFORMATION BROKER.



Participant roles within a transaction include:

- Information Producer - the entity that has drafted a piece of information for publication
- Information Provider - the entity that is publishing the information to the repository. This may not always be the same as information producer in the cases where the producer would like to stay anonymous
- Information Consumer - all entities that have consumed a piece of information.
- Information Broker - an entity that negotiates between two or more entities arranging for the publishing and consuming of information

> "Information brokering is a pragmatic means of knowledge exchange: ..., knowledge cannot be exchanged directly. However, knowledge can be externalised and re-conceptualised (i.e. transformed into information) and then exchanged as information. At the receiving party, the delivered information can then be turned into knowledge by contextualisation again." [16]

Clearly defining participant roles allows for a bounded exchange of information, holding each participant to pre-defined rules when acting in that role within the defined cyber defense sharing network.

When describing an Information Broker, an organisation may explicitly choose to be a primary information broker within a network so that it gains the widest and deepest view of network knowledge. However, organisations may only become a trusted information broker when the level of perceived trust with that organisation is sufficiently high enough across participating organisations such that that organisation brokers the flow of information between participants that do not have a high enough perceived trust between each other.

Governance Structure

The governance structure of a cyber defense sharing network within an information sharing environment must address two distinct areas:

First, there is the governance structure of the network participants:

- how participants are structured (e.g., defined roles and responsibilities)
- what are the duration, participation and interaction types,
- what sharing network membership and usage rules are in place to handle day to day activities and address dispute resolution between participants,
- what kind of trust-building policies are in place to encourage success.

Governance also addresses the information sharing relationships between participating entities. Specifically, it is a description of the top cover needed by sharing entities to ensure each producer and consumer is empowered by their management to share specific types of information.

FIGURE 3. PPP INFOGRAPHIC FROM ENISA PAPER

Using ENISA's publication on Preliminary Taxonomy for Public-Private Partnerships (PPPs) [6] as a guide to governance structure, we will walk through each component, specifically focusing on the incentive impacts for each component.

Organisation

The ENISA paper [6] references the Milward and Provan model on collaborative networks where all networks are describable using three constructs: run by one from within, run by a coordinating entity, and democratically peer led. We have conducted an initial set of interviews with members of two incident response teams and our preliminary research indicates that the most successful cyber defense information sharing model is the democratically peer led network where individual trust relationships tend to increase the amount of sharing that takes place. From what we have also observed partnerships that have a "run by one from within" structure tend to form more quickly but later fail to gain traction.

Roles and Responsibilities

The roles and responsibilities within an information sharing network can be non-exclusively tagged to these taxonomy categories: Chaired by {elected representatives from Industry, representative from Government}, Secretariat supplied by {third party (non-government), national government}, and Co-ordinated by {government, industry and collectively). When the information-sharing network is very large, roles and responsibilities help to organise the community and maintain a common understanding of relationships and expected contributions from participants. Roles and responsibilities also help to clarify the goals of each participant for the community.

Duration Type

Governance structure and institutional funding are both impacted by the duration type of the sharing network. Some sharing networks are classified as persistent community groups, setup to serve a community of interest without a bounded endpoint. A second classification bounding the duration type of a sharing network is a working group where specific problems are addressed and the group is disbanded once objectives are met or the group is disbanded. The third duration type classification is a rapid response group that is more or less an extension of the working

group in that the sharing network is created to address an urgent issue and may only be in existence for a matter of hours or days.

Participation Type
Participation dynamics within sharing networks are interesting from the perspective of both corporate governance as well as individual motivations. A successful sharing network may only succeed by providing entry-points for all types of participants. Participation can be in the form of a subscription where a participant pays a fee (or just subscribes) to a sharing network to gain access to the collective knowledge. While subscription based services describe a mechanism for interacting with sharing networks, two other participation types describe a commitment level for participants, either mandatory or volunteer. Mandatory participation may be leveraged upon an individual or organisation by the owning entity such as a government. Voluntary participation may, on the other hand, incentivise a participant to use the information sharing network since they may wish to shape their participation based upon their organisational or operational priorities.

Interaction Type
The ENISA PPP paper [6] outlines two interaction types: face-to-face and virtual cooperation. This is largely an extension of the time/place collaboration square where sharing mechanisms vary according to the location of participants and the length of interaction. Governance structure will often dictate the interaction type but successful interaction within a cyber information sharing network will often be based upon the duration type (severity of engagement).

Formal Information Usage Agreements
Information which is shared in a cyber defense sharing network must be protected. This requires a legal component – who is the information owner, how can the information be used, can it be attributed to the owner, etc.

Trust Building Policies
Building trust has two components. First, participants will develop trust in the cyber defense sharing network as participants feel that the information they contribute is protected (e.g., the network should be able to provide anonymisation for contributed data), and that the network provides them the opportunity to gather valuable information unavailable elsewhere, providing high value back to participants (e.g., bringing in participants with expertise that incentivise new members).

Second, participants will develop trust in each other over time as their relationships strengthen. In our experience, holding face-to-face meetings throughout the year significantly increases trust building among participants. Highlighting shared goals and facilitating partnerships among participants to realize these goals will also go a long way to building strong trust and partnership in a cyber defense sharing community.

Establishing Collaborative Processes
The multi-dimensional view of information sharing transactions requires a defined collaborative process. This defined process also helps to alleviate the anxiety of a transaction by providing to

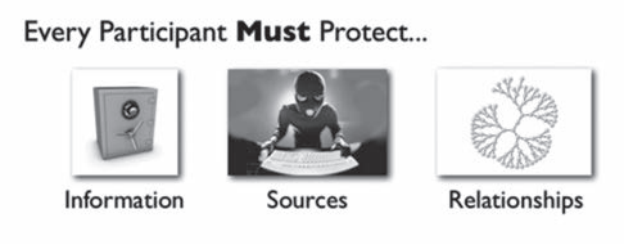
each party a set of steps, responsibilities and time-to-act deadlines to facilitate the information exchange.

Information Protection and Release Control

Often we will see information sharing partnerships fail not because the two parties do not trust each other to have the information, but one party may doubt the other party's ability to protect information consumed appropriately. This is especially true in the case of classified data that may pass between nations or cyber threat signatures that if an adversary knew existed would allow for crafting of attack payloads that do not trigger (at least for that rule set) an alert.

The procedural model must include steps for protecting information as it is created, published, consumed, stored and eventually destroyed. The information exchange platform must itself be capable of protecting all information it stores from unauthorised access.

FIGURE 4. IPRC INFOGRAPHIC



Incorporating Financial Incentive Models

Within the malicious software community exploits are bought and sold based upon the perceived value of the exploit. Is it something that no one else even knows about? Does it affect a piece of software used by your targets? Is the author someone you can trust to have not sold the exploit to anyone else already? Does the asking price match the perceived value? Existing research, for example [18], shows that information-sharing networks need to incorporate these types of financial incentive models into their procedural underpinnings. Approaches as Worldwide Intelligence Network Environment (WINE) [7] could help to build financial incentive models. Not every network participant will bring the same capabilities to the table, therefore there may need to be a financial incentive in place in lieu of reciprocal information exchange such that those who have valuable information to share aren't vested because their return is not sufficient.

5. AUTOMATION OF SHARING MECHANISMS FOR TECHNICAL CYBER DEFENSE DATA

The need for automation and standardization of cyber defense data is apparent in the government, academic, and industry sectors on an international level. Information sharing that can relieve the human workload is necessitated by the sheer speed of cyber threats today. Standardization of data to be exchanged provides an effective pathway for information sharing between multiple parties, because the format of the data is then agreed upon. Standardization

also lends itself to automation of information sharing, and both lower the bar for entering into a cyber defense data sharing network.

Trust is a very important component in regards to automated information sharing. When the speed at which data could be shared increases, the risk of sharing information with unauthorized parties is raised, potentially backfiring and creating a disincentive for participation in an information sharing network. Nonetheless, the existence of an automated exchange can provide an incentive for joining the network; automation increases the benefit the parties involved by receiving data quickly and eases the process of contributing data to the network.

Additionally, the details of the sharing relationships and the automation involved depend heavily on the type and sensitivity of the information to be shared. Some information types are considered high-risk in sharing environments; they would reveal too much sensitive data and existing initiatives are faced this challenge as Sharemind [7,9]. Low-risk data, or data of less sensitivity, is more likely to be shared in an automated information exchange. It is important to keep in mind that the level of trust of the partners and the level of sensitivity of the data are directly related.

The data in a cyber-information sharing network could include the following types:

- Vulnerability information
  - Vulnerability existence checks
  - Related patches and mitigations
  - Quality of service effects
  - Vulnerability Assessment tests/results
- Threat actors
  - Names/pseudonyms
  - Countries of origin
  - Common methods and tactics
  - Attack patterns
  - Events and incidents
  - IDS Signatures
  - Implicated parties
- Black or white list information (IP addresses)
- Software
- Hardware
- Malware
- Protocol specifications
- Security configurations
- Security guidance
- Weakness information, patch remediation
- Secure coding practices

Of the above types, high-risk data may include specific threat actor information, especially attack patterns and methods. Internal security configurations are also high-risk. This is because

they can reveal sensitive information about the organization and may be shared with a party that is not trusted with that level of sensitivity. However, blacklist information, security guidance, or patch information may be considered lower risk, and are appropriate for an automated exchange without an exceptionally high degree of trust. Information sharing networks and the number of participants actively involved will most likely be directly related to the amount of data available. Since high-risk information is less likely to be shared, a low-risk sharing environment may create the best incentive for participation.

One example of an automated cyber defense-sharing network (including exchange of many data types) is CDXI (Cyber Defense Data Exchange and Collaboration Infrastructure) for Cyber Defense data exchange, a system being built by NATO [14]. CDXI will serve as a repository for participants worldwide (individuals, organizations, non-NATO entities, industry, government, and academia) that will automatically push and pull cyber defense data using a variety of Application Programming Interfaces (APIs). Quality assurance of data and data confidentiality are integral to the CDXI design, and in order to achieve the right balance of information protection (i.e., sharing with appropriate parties) and openness of the network, confidentiality and access control are implemented based on user, role, and NATO classification level.

CDXI data is to be structured for machine processing and automation but also have a human-readable component. Automatic exchanges exist for some of these information types, however in practice much of this information (such as configuration information and operational events) is exchanged via prose documents and requires manual interpretation and implementation. Automating the exchange of this data should likely increase efficiency, which not only increases the incentive to share and participate in the information sharing network, but also saves valuable time in securing an organization against fast-acting threats.

Automation, however, requires standardization of data before it can be automatically exchanged. An agreement between parties on the format of data is often required in order to exchange, so standardization in and of itself can provide an incentive for information sharing. One popular example of a data standardization protocol is the Security Content Automation Protocol (SCAP). SCAP includes a suite of standards that provide a common way to identify vulnerabilities (Common Vulnerabilities and Exposures or CVE), platforms (Common Platform Enumeration or CPE), and configurations (Common Configuration Enumeration or CCE), as well as a common way to express configuration information and security guidance (eXtensible Configuration Checklist Description Format or XCCDF), system configuration and vulnerability assessment (Open Vulnerability and Assessment Language or OVAL), and vulnerability risk (Common Vulnerability Scoring System or CVSS). These internationally accepted security standards encapsulate valuable vulnerability information and are widely used across government, academia, and industry.

The National Vulnerability Database or NVD is a freely accessible repository for SCAP data such as NVD contains CVE vulnerability feeds with CVSS scores, the CPE product dictionary, CCE reference data (and soon a vulnerability feed), and NCP (National Checklist Program) checklist feed. These checklists are usually a bundle of data including at least an XCCDF-expressed checklist, but also may be annotated with CVEs, CPEs, or CCEs and may include

OVAL definitions or other automated checking mechanisms. Each of these feeds is available in an RSS or XML format.

The NCP checklists are presented in tiers. The most important tiers for automated standardized data are Tiers 3 and 4. Tier 3 designates data that should work in an SCAP-validated tool (i.e., passes SCAP data stream requirements but may need to be tested), and Tier 4 designated data that does work in an SCAP-validated tool (i.e. passes SCAP data stream requirements and has been tested). While the contributors to these tiers have been primarily been government or government-contractor organizations (e.g. NSA, DISA, MITRE) there are a few examples of private companies that have adopted SCAP data formats and contributed content, forming a public-private partnership. Microsoft has been very involved in expressing its configuration information in the SCAP format. For example, Microsoft's SCM (Security Compliance Manager) now provides extensions to express configuration information in SCAP format. Additionally, Microsoft provided the Tier III Checklists to the NVD on a total of 12 platforms, including several versions of Windows operating systems, Office, and Internet Explorer. CyberESI is another private company that has contributed to the National Vulnerability Database using SCAP-formatted data. CyberESI is an information security company that provides services to both government and commercial clients. CyberESI developed a Tier 3 checklist that checks for suspicious filenames and locations on a Windows XP system. While they have not contributed to the NCP, Red Hat now includes in all of their security updates with OVAL definitions that check for the vulnerability or configuration issue. These are only a few of the major private contributors that have shared information in the standardized SCAP format.

In terms of information sharing networks, these databases provide an automatic yet mostly one-way trusted flow of information. While it is two-way in the sense that community members (which include government, academia, and industry) may provide the information to be vetted by NIST or MITRE, it is one-way to the largest population of users: the public. Since these websites are public and the total community of users is not controlled, they lack some of the ideal characteristics for a highly utilized information sharing network. However, the automatic ability to pull data in each case account for both repositories' reputation in the field of vulnerability and security configuration data, and may indirectly contribute to the volume of data (49,000+ CVE IDs, 7500+ OVAL queries and 220+ checklists) by creating a strong community of users. The important lesson to learn from these repositories is that when many parties, with many different ways of describing and expressing their data are trying to exchange non-standard information, the information can't be normalized. An important issue to consider, however, is how standardization is applied. For example, the success of CVE spawned the growth for many more security-related standards, but few have the widespread success that CVE did. Research [5] that examined why some standards are more successful than others found that differences between machine- and human-oriented standards contributed to a standard's success, and that this must be considered when using or developing standards for information sharing environments. In particular, standards that include little detail (e.g. a CVE ID), allow for a greater degree of diversity in the information represented, while a very detailed (i.e. more constraining) standard will result in very similar enumerations. This is an important consideration depending on the type of data to be shared in a particular environment.

Repositories with more sensitive information require collaborative trust to incentivize potential new users. One example is the U.S. Defense Security Information Exchange (DSIE). DSIE is an information exchange network for U.S. Defense Industrial Base (DIB) companies to share information on cyber-related events and attacks, formed in 2008 [12]. In order to facilitate sharing, DSIE members sign a Non-Disclosure Agreement (NDA) which states that all information is non-attributional and that only DSIE members can view the information.

Cyber information sharing networks with high participation will ideally contain a large amount of data. The collection, processing, and distribution of this data in the network are time consuming if done primarily manually. Automation of the exchange data is important to consider in the network. Automation may increase the incentive to join the network, share information, and continue to be an active user. Standardization plays an important role, since it is a prerequisite to data automation in some way. How standardization is used and applied depends on the data to be shared and its usage. Other considerations include the risk-level of automatically shared data and pre-existing trust relationships. While the technology and procedures around standardized and automated cyber information sharing must be carefully considered, standardization and automation ultimately provide a great incentive for sharing by reducing manual work and increasing efficiency.

6. CONCLUSIONS

Research into the field of incentive networks, specifically collaborative scenarios for sharing information within trust relationships, is still quite new. Throughout this paper we have presented a common sense approach for thinking about how incentives in sharing networks work. We started with identifying incentives and barriers for information sharing. We looked at the importance of modelling the networks for information sharing (the aim of the network, the goals of the participants, and the envisaged benefits and challenges of each participant to establish the principles and the procedures that rules the network) and then moved onto the idea of collaborative risk management models and the important notion of information value perception.

Once a clear common understanding is achieved with regards to these kind of networks, procedural models for improving data exchange will help to start driving an organisation towards integrating their risk models with their information sharing models such that an agreement of threat level, envisaged impact, risk methodology and finally mutual aid from a risk management point of view will help to improve the effectiveness of the collaboration network.

Over the next few months we will continue our research into sharing networks and incentives with the intent on providing a more thorough review of our research at the CyCon 2012 Conference this June in Tallinn.

REFERENCES

[1] ENISA. “Incentives and Challenges for Information Sharing in the Context of Network and Information Security”. September 2010.

[2] Bodeau, D., Powers, E., Brooks, J. Making Sense Together: Applying Ethnomethodology to Enhance Advanced Systems Engineering in the Information sharing Domain.

[3] NIST sp-800-53 Recommended Security Controls for Federal Information Systems. April 2009. Retrieved January 2012 from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[4] ISO/IEC 27005 Information technology - Security techniques - Information security risk management

[5] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Retrieved January 2012 from http://administracionelectronica.gob.es/?_nfpb=true&pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

[6] ENISA. “Cooperative Models for Effective Public Private Partnerships. Desktop Research Report”. Retrieved January 2012 from http://www.enisa.europa.eu/act/res/other-areas/national-public-private-partnerships-ppps/desktop-reserach-on-public-private-partnerships/at_download/fullReport

[7] Dumitras et al. in “Toward a standard benchmark for computer security research: the worldwide intelligence network environment (WINE)”, BADGERS’11, 10 April 2011, Salzburg, Austria.

[8] Bogdanov, Dan., Laur, Sven., Willemson, Jan. Sharemind: a framework for fast privacy-preserving computations. In Proceedings of 13th European Symposium on Research in Computer Security, ESORICS 2008, LNCS, vol. 5283, pp. 192-206. Springer, Heidelberg (2008).

[9] Talviste, Riivo. Deploying secure multiparty computation for joint data analysis — a case study. Master’s thesis. University of Tartu, 2011.

[10] Mann, D., Brookes, J. Information Standards and Their Use: Implications and Design Patterns. March 2010.

[11] P. Welsh, “Newest version of DCGS Integration Backbone improves intelligence sharing”. Retrieved January 2012 from http://www.afmc.af.mil/news/story.asp?id=123228659

[12] “Defense Security Information Exchange (DSIE) A partnership for the Defense Industrial Base”. Retrieved January 2012 from http://www.whitehouse.gov/files/documents/cyber/Defense%20Security%20Information%20Exchange%20-%20DSIE%20summary%20-%20William%20Ennis.pdf

[13] ENISA. “United Kingdom Country Report”. May 2011. Retrieved January 2012 from http://www.enisa.europa.eu/act/sr/files/country-reports/UK.pdf

[14] L. Dandurand, “Cyber Defense Data Exchange and Collaboration Infrastructure (CDXI)”. ITU-T Workshop December 2010. Retrieved January 2012 from www.itu.int/dms_pub/itu-t/oth/06/35/T063500000200516PPTE.ppt

[15] NATO Consultation, Command and Control Agency Reference Document RD-3060, “CIS Security (Including Cyber Defense) Capability Breakdown”, G. Hallingstad, L. Dandurand, NC3A, The Hague, Netherlands, November 2011 (NATO Unclassified).

[16] R. Klemke. “Modelling Context in Information Brokering Processes”. Retrieved January 2012 from http://darwin.bth.rwth-aachen.de/opus3/volltexte/2002/381/pdf/Klemke_Roland.pdf

[17] The semantic web with information broker. Retrieved January 2012 from http://www.semanticweb.org/

[18] Golle, P., Leyton-Brown, K., Mironov, I., and Lillibridge, M. “Incentives for Sharing in Peer-to-Peer Networks”. Proceedings of the 3rd ACM Conference on Electronic Commerce, New York, NY. 2001.

[19] G. Hallingstad, L. Dandurand, NATO Consultation, Command and Control Agency Reference Document RD-3060, “CIS Security (Including Cyber Defense) Capability Breakdown”, NC3A, The Hague, Netherlands, November 2011 (NATO Unclassified).