Out of the Trenches

Creating Standards to Share Wisdom and Knowledge

Andrea Rigoni

Protection of cyber space is this era’s big challenge. All of the main critical infrastructures and core business activities of private organization are interconnected. Intrusions into infrastructure such as electrical grids, financial services, and transportation could affect the social and economical stability of an entire nation. Furthermore, over the course of the last few years, the frequency and complexity of cyber attacks is growing. Globalization has led organizations around the world to use the same technologies, resulting in the sharing of vulnerabilities and the creation of critical interdependencies. A threat could have horizontal effects that impact many organisations.

Due to the specific nature of Internet, and modern information and communications technology (ICT), public and private organizations have a limited and fragmented vantage points. They have a “trench view” of cyberspace. Because of this their defense and protection capabilities are limited.

Information sharing could allow these organizations to move to a “satellite view,” improving protection and increasing their cyber security postures. Despite the fact that it is very apparent that information sharing is beneficial to cyber security, there are very few successful examples of this trend,
in particular between public and private actors. Information sharing not only aids parties in establishing collective perspectives on the threat, but it also helps organizations in coordinating basic approaches and countermeasures on cyber security. Too often a common obstacle to cooperation is the lack of a mutual understanding on cyber security. To coordinate, the entities need to speak the same language, use the same terminology, and have shared basic concepts.

**Information Sharing Matters.**

Information has always been vital to national security, and information sharing is a key activity of intelligence and defense. In war, accurate and timely information is essential in carrying out a military operation. Additionally, having an advantage over the enemy in peacetime can prevent incidents of national impact. This is a key element of the modern defense doctrine known as "Network Centric Warfare" or Network Enabled Capability. The main difference between the present and the past is the capability to share information and the increase agility thanks to "shared situational awareness." Information is now shared at various levels through robust networking.

The foundation of this doctrine is that information sharing enhances the quality of information and shared situational awareness, shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command, and these dramatically increase mission effectiveness.

The quality of the information shared is increasingly high. Information shared is reliable and in many cases complete and timely. This allows the organization to have a real-time view of threat scenario and have available the relevant information to identify the best preventive or corrective measures to adopt.

Recently in the United States the Cyber Intelligence Sharing and Protection Act (CIPSA) has been proposed to regulate the sharing of cyber threat intelligence and cyber threat information between the intelligence community and other entities.

In 2003 the Department of Homeland Security issued Presidential Directive 7 (2003) that mandates the public and private sectors to share information about physical and cyber security threats, and vulnerabilities to help protect the U.S. critical infrastructure. In response, many Information Sharing and Analysis Centers (ISACs) for specific sectors were born such as ES-ISAC for electricity sector through timely, reliable and secure information exchange, ICS-ISAC specific for Industrial Control System, or FS-ISAC for collaboration on critical security threats facing the financial services sector.

Information sharing is not only a key element of modern defense, but also of many civil sectors. Information sharing is vital to operating electric networks, financial services and stock exchanges, transportation, and much else. Because of all of this, it becomes increasingly crucial to craft standards that ensure that quality information is shared and
Theories of Information Analysis. In 1989 Russel Ackoff, a system theorist and a professor of organizational change, elaborated a model to describe the content of the human mind, defining five categories: data, information, knowledge, understanding, and wisdom. Ackoff is considered the father of modern knowledge management, as we know it in ICT. A simplified model has been adopted in intelligence and defense called the DIKW pyramid. The model considers knowledge as a pyramid of four levels. The base of pyramid is composed of data. Data is raw. It simply exists and has no significance beyond its existence. It does not have meaning of itself. Information is data that has been given meaning by way of relational connection, provided by the context. Information processed, organized or structured in some way, or applied or put into action become knowledge. Finally, the use of knowledge and experiences creates wisdom. Wisdom is therefore the process by which we also discern, or judge, between right and wrong, good and bad.

Information sharing is not only a key element of modern defense, but also of many civil sectors.
wisdom, deals with the future because it incorporates vision and design. With wisdom, people can create the future rather than just grasp the present and past.” In fact, the wisdom tier helps to identify the best choice.

**From Theory to Application.**
The DIKW pyramid can and should be applied to how we think about cyber security. We collect huge amounts of data from firewalls, Intrusion Detection Systems, antivirus, network devices, access points. Though their analysis, we can gather information about events and intrusions. Through the context and human analysis, we are able to know what happened (incidents) and through additional analysis we can understand why it happened (threats and vulnerabilities). Wisdom helps us to define what could happen in the future and how to avoid it. In cyber security we could couple wisdom with “lessons learned.” Wisdom can help us define guidelines and standards in order to prevent future intrusions and attacks.

ISACs in United States – are mainly focused on sharing knowledge through face-to-face meetings or round tables.

Despite the intent of many organizations to exchange information and data, they fear sensitive information may be made public and cause damage to their image, or favor their competitors. Others lack a culture of sharing, and they appeal to legal and security policies to avoid it.

Another factor limiting the development of information sharing in cyber security is that in many countries most of the interesting data falls under local data protection law. This is particularly true in Europe, where not only personal information, but also any other data that combined together could represent to “personal information” cannot be shared. Logs of systems and devices, for example, could contain end user data (web or email logs) and therefore cannot be shared outside the organisation that collected the logs unless there is the consent of the end user.

Despite these limitations, the shar-

**Despite the intent of many organizations to exchange information and data, they fear sensitive information may be made public and cause damage to their image, or favor their competitors.**

Standards resulting from international cooperation between many different experts and stakeholders exist. Most of information sharing in cyber security is currently focused on the data and information tiers, and not on the higher levels. The most successful initiatives — such as the Information Exchanges in United Kingdom or the
We need an initiative where public and private actors are both involved, bringing together experts from critical infrastructures, defense, government, academia, and industry.

oped to transfer data between systems as http (hyper text transfer protocol, used for the web), smtp (simple mail transfer protocol), ftp (file transfer protocol), dns (domain name system), to the more sophisticated ones used for specific applications as power plant and generator monitoring, and control or for exchanging air traffic control traces.

The first attempt to stimulate information sharing in cyber security through a standard is the ISO/IEC 27010 published in 2012. It is a specific standard for information sharing that defines a framework to help both public and private organisations to share knowledge and information on cyber security. This standard provides guidelines in addition to guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities. It provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organizational and inter-sector communications, and it is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors. The standard provides in its annexes the same implementation examples as the Trusted Information Communication Entity (TICE) and the Warning, Advice and Reporting Point (WARP) – two common models that can be used to create supporting entities or the Traffic Light Protocol (TLP) mechanism widely used in information sharing communities to indicate the permitted distribution of information.

Climbing Out of the Trenches.

Even if many tools and techniques such as the ISO27010 are available, most organisations around the world are still not involved at all in any form of information sharing. Even those countries that are promoting national information sharing are hesitant in practice, as they fear that it could increase vulnerability instead of reducing it.

A potential solution to promote sharing in the international arena is to “climb” to the next level of the DIKW pyramid and prioritize sharing knowledge and wisdom over data and information. This new level of sharing could bring many benefits and allow an easy start-up of an international cooperation on cyber security.

Standards are the results of wisdom. Organisations could work together to share new controls and practices to define or improve cyber security standards. Participants will benefit of common practices, methodologies, technologies, policies and procedures, without fearing of exposing their respective
organisations. Results of such activity could be easily shared with other participants in different sectors or countries. This model is not new at all. It reflects the manner in which most of the technical and procedural standards were born. Experts from different countries and organisations have been working together for centuries in defining every kind of standard from telecommunications to electricity, from transportation to Internet.

Why do we need a new initiative when we already have developed institutions like the ISO Subcommittee on Information Security? We need an initiative where public and private actors are both involved, bringing together experts from critical infrastructures, defense, government, academia, and industry. CERTs (computer emergency response team) and National Cyber Security Offices could work together to establish an initiative to define and share standards with their counterparts in other countries, creating specific working groups focused on different sectors. This process could start between like-minded countries that are already willing to cooperate on cyber security.

NOTES

2 For more information see: http://www.esisac.com/SitePages/Home.aspx
3 For more information see: http://icscybersecurity.wordpress.com/ics-iasac/
4 For more information see: https://www.fisac.com
10 Ackoff.