A Multidisciplinary Analysis of Cyber Information Sharing

Aviram Zrahia

The emergence of the cyber threat phenomenon is forcing organizations to change the way they think about security. One of these changes relates to organizations' policy on sharing cyber information with outside parties. This means shifting away from the view of the organization as an isolated, compartmentalized entity towards a view of the organization as a sharing one. Sharing generates a complex, multifaceted challenge to technology, law, organizational culture and even politics. Establishing a system of sharing serves many parties, including regulatory bodies, governments, legal authorities, intelligence agencies, the manufacturers of solutions and services, as well as the organizations themselves, but it also arouses opposition among elements within the organization, and organizations defending the right for privacy. The purpose of this essay is to present the various challenges posed by cyber information sharing, expose the reader to its conceptual world, and present some insights and forecasts for its future development.

Key words: cyber, information sharing, privacy, regulation, information security, trust

Introduction

One of the most difficult challenges faced by organizations is confronting the cyber threat phenomenon. The increased use of technology in organizations of any kind–government, public, and private–turns them into targets of attacks aimed at gathering or damaging information, or suspending services. Attacks on commercial organizations are liable to harm the organizations'

Aviram Zrahia is a cyber security expert at Juniper Networks and a lecturer on cyberspace, and is an intern at INSS.

reputation, endanger physical assets and intellectual property, and cause serious financial damage. Attacks on governments, public bodies, and infrastructures may also disrupt the routines of entire nations and jeopardize the health and safety of their citizens.

Over the last decade, traditional crime has crossed into cyberspace; the growing sophistication of cracking tools and attack vectors has led to the creation of a new, developed and sophisticated cyberspace crime economy. A similar process has also occurred in the sphere of warfare between nations, as many now view cyberspace as the fifth dimension of the modern battlefield, in addition to sea, land, air, and space.

Confronting the cyberspace threat requires an investment in human and technological infrastructures based on an organizational or national risk management policy. The quality of an organization's information security system is affected by different factors, among them the ability to gather and analyze information on legitimate user traffic as well as attacks, regardless of their success. This allows one to identify vulnerabilities in the security system and prevent their exploitation, while identifying and responding to attacks and breaches quickly and effectively, thereby preventing or at least minimizing the damage.

Sharing organizational cyber information is the act of communicating information regarding an organization's security to an external party. While such sharing results in gains for both parties, it does, however, create a complex, multifaceted challenge and represents a shift in the traditional information technology paradigm. The sharing model may exist within the same sector, across different sectors, between commercial enterprises and government bodies, and between different governments. The last two years have seen an increase in the sharing trend; regulatory and law enforcement bodies, both local and international, are promoting it by means of incentives, guidelines and legislation. Concurrently, a security solutions industry based on information sharing among bodies is developing rapidly.

The purpose of this essay is to present the multifaceted nature of the challenge posed by sharing. It begins by presenting the current state of affairs and related problems, followed by an analysis of the practical aspects of sharing implementation, including reference to the theoretical background of trust among bodies. The following section lists the organizational gains and challenges, describing the business opportunities, aspects of the law, regulation and privacy. The paper concludes by offering several insights.

Most of the examples in the essay are from the United States, where sharing initiatives, standardization efforts, government and intelligence agencies actions, and legislative processes are open and at the heart of public debate.

From Compartmentalization to Sharing

The cyber threat is a sophisticated, complex dimension of crime and warfare that has developed in recent years in scope and severity. In terms of the scope of the threat, organizations must now defend not only their computer networks and information systems but also the range of endpoints available to users, such as smartphones and tablets, as well as infrastructure systems, including electricity and air conditioning. They must do so continuously while also making sure they can provide service anywhere, anytime, as expected of an organization of this era.

In terms of the severity of the threat, attacks are becoming harder to identify and locate, as they also include undocumented attack vectors that are unknown to the manufacturers of security solutions. This is true of zero day attacks;[1] the fact that hackers share information continuously and in real time creates a situation in which any weak point exposed in the system or malware can be replicated and used as means to perpetrate an attack almost instantaneously, regardless of location. A recent study of the topic conducted by the RAND Corporation[2] provides an analysis of the way in which cyberspace black markets are built, functioning like ecosystems with clear infrastructure and modules.

These developments create a paradigm shift towards joint efforts at fighting cybercrime, and as a result, many organizations are changing their approach to security; in most organizations, except for those subordinate to regulation and military and/or government systems, the approach to information security management was characterized by total separation from other organizations, both in terms of the technology of their information and security systems and in terms of sharing information about cyber events and security. Information about an attack or an attempted attack and the results of its analysis were kept within the organization, classified and distributed to a very limited intra-organizational list. Revealing information to a third party was perceived as a risk, a move liable to result in damage to its reputation, legal exposure and other complications.

Recently, this trend has reversed. Many organizations and authorities have abandoned the compartmentalization strategy[3] in favor of information sharing. Through sharing cyber information among organizations, the way hackers do on the attacking side, security measures created in a certain organization to deal with a particular threat can be used by other organizations as an inoculation or at least as information that will heighten their alertness to that particular threat.

The high costs incurred by organizations–in terms of time, manpower and technology–required to provide an effective security protection generate an organizational interest in sharing information and passing some of the costs on to a third party. A study carried out in the United States[4] analyzed the connection between sharing cyber information and the costs of organizational cyber security. It found that companies sharing information spent less on security systems to reach the same level of protection attained by companies that did not share information, meaning that companies can save on direct costs as a result of information sharing. This includes, for example, proactive intelligence gathering and input about weaknesses and expected attacks, inoculations to attacks that occurred in other organizations, use of professionals to help analyze security events, and more.

Another reason for the change in organizational approach to information sharing is the direct and indirect business value in meeting standards and regulations. In certain critical sectors, like finance, healthcare, energy and communications, even private organizations are required to allow state supervision. Most regulations demand information sharing between the organization and some oversight body when it comes to cyber events or attempted attacks. In addition to the obligations, the regulations may have direct and indirect value: a financial organization subject to the Basel III regulation[5]–a standard relating to financial institutions requiring transparency on security events vis-à-vis the regulatory body–enjoys the direct benefit of improved capital allocation for the credit it extends, creating a greater profit margin. An example of indirect benefit may be found in an organization providing services that can make a bid on a government tender that requires bidders to meet the ISO-27032 standard,[6] which also entails information sharing.

Technological Principles in Information Sharing

Secure information sharing among organizations is, in many ways, a technological and operational challenge, from goal and policy articulation to implementation and use. The methods required to meet the challenge must balance many different components: the ability to support a very large range of organizations and easily add them to the sharing endeavor (scalability); the ability to make use of information after establishing correlation and analyzing it in close to real time so as to produce maximal benefit (usability); and a system of controls to ensure the existence of the "CIA" principles: confidentiality, integrity, availability.[7] The steps towards constructing a system of sharing must include, among other things, goal articulation and participant definition, the privileges and obligations of the participating organizations, technological architecture, trust and oversight model, and work processes.

Information sharing among different entities requires the creation of a system of trust in order to ensure that the information is correct, complete, beneficial and useful. Trust is the basis for all the practical models and examples discussed in this essay. When it comes to trust, the sphere of discussion and solutions ranges from a product's components such as a computer, through the incorporation of various products into a system, to the trust between different systems in different organizations, such as, for example, internet commerce. Standards institutions, such as the Trusted Computing Group,[8] deal with many aspects of the topic, but cyber information sharing is a challenge for which the existing models have not yet provided a complete answer, hence the need for separate debate and the establishment of standards on this point precisely.

When building infrastructure for information sharing, there are three possible models.[9] The first is the "hub and spoke" model in which a central site receives information from the end organizations, fuses it to accommodate different needs and then disseminates it.[10] The hub serves as a clearance center protecting privacy and the intellectual property of all the participating organizations; its use is made possible in part by the accelerated technological development in the field of big data. This allows the processing and analysis of tremendous amounts of information and is a basic building block in constructing the ability to fuse information from different sources. The drawbacks of this model are primarily the consequences from its centralization: the challenge of size, dependence on a central site, delays in processing and disseminating the information.

The second model is the post-to-all architecture in which information is directly distributed among the participating organizations. Since the data distributed is raw, this model requires infrastructure for analysis in every organization. The third model incorporates aspects of the first and second, striving to take advantage of the relative strengths of each. However, it is relatively complex and expensive to implement.

Technologically speaking, realizing the goal of sharing must take into account protecting an organization's assets and privacy in two ways: first, control of the information being shared based on the participants' goals, and a standardized agreed-upon format. Some of the definitions are meant to conceal the true sources of the information–as in the field of intelligence gathering– so that unnecessary details do not leak outside the organization. The second way entails limiting access to the information, and includes control of its distribution, where it is sent and who sees it, and must be based on a standardized sharing protocol.

Another fundamental choice that must be made is between the automated sharing model and the manual sharing model. Manual sharing means that an authorized party within the organization with access to the sharing system sends and receives information, and controls access to the information. The manual model has a prominent drawback: the human factor creates a bottleneck, especially when the organization is under attack. Other drawbacks include human error and difficulty of managing constant updates.

Automated sharing forces one to decide on a uniform, normalized format, a system of sensors in the organization that will gather and disseminate information, a monitoring system for local reception of warnings, and meticulous realization of controls designed to prevent unwanted distribution of sensitive information. This method overcomes the limitations of manual sharing, but it requires organizations to confront attack scenarios in which the automated sharing system is exposed, such as database poisoning.[11]

Some cyber information sharing standardization activities are already taking place. The most advanced, which has also been adopted by the US Department of Defense, involves a format called the Structured Threat Information eXpression (STIX™).[12] This format defines the structure of a database in which information relating to a user and/or traffic is proactively sent from the organization to an external entity or from an external entity to the organization while containing a range of structured details about a security event. Another relevant standardization for automating sharing is called Trust Automated eXchange of Indicator Information (TAXII™),[13] and it contains the structure of messages and network protocols supporting the transmission of STIX-type messages among different entities. There are several other peripheral protocols under a wider architecture called Cyber Observable Expression (CyBOX),[14] supported by the US Department of Defense as part of the effort to automate sharing.

It seems that most theoretical models suggested by academics[15] and the practical models suggested by various research institutions[16] are based on automated realization, trust, and a "hub and spoke" sharing architecture. The standardization efforts referred to above suit the spirit of the academic and practical models, so that it seems that, technologically, there is a consensus over the right way to construct such a system. And, indeed, significant parties, such as the US Department of Defense, are working to advance projects based on this outline.[17] Nonetheless, the road to realizing effective information sharing remains long because of the multiple technological, commercial, operational, legal, and (some would claim) moral challenges faced by the sharing initiative members.

Benefits and Risks in Information Sharing

The value of sharing differs depending on the interests of the parties involved. In the case of commercial enterprises, sharing allows a heightened level of security and a reduction in response time in case of an attack, or inoculation against a possible attack in the future by means of receiving warnings and help in identifying, analyzing and confronting attacks. An experiment carried out by a South Korean research team supports this assessment.[18] Sharing also facilitates a reduction in the cost of security thanks to at least partial outsourcing of the analysis and response to a third party. Furthermore, the organization can benefit from regulatory relief as the result of increased transparency and meeting reporting obligations and other conditions.

In the case of the vendors and solutions and services providers, this is a new, technologically-oriented market segment with great growth potential that can distinguish them by creating sustainable, competitive advantages. One of the primary services this sector can offer is identification of possible attack patterns and the distribution of inoculations and warnings to organizations on the basis of fusing information about attacks and attackers gathered from the organizations themselves.

In the case of governments, it is in the interest of regulatory bodies and government and intelligence agencies to encourage sharing because they increase the organizations' transparency, receive a broad situation assessment of the availability of services and credibility of the information, undertake analysis across different networks and organizations to identify patterns of attacks that have taken place or might take place, and allow for the possibility of a rapid response while disseminating the information to other organizations for the purpose of inoculating them. A state-sponsored body has the ability to construct and maintain a high level of technological capability for its personnel, and to cooperate with organizations in terms of human and technological resources. Sharing is an obvious national interest, allowing the government to fight the national cyberwar and strike at cybercrime in the most effective way possible as well as control the availability of critical national, public and private infrastructures. An example of the realization of regulation with a similar orientation in a different field may be found in regulations on the emission of industrial pollutants, which in some countries require industries, continuously and online, to monitor and report data on air quality in chimneys and other sources of pollution.[19]

Despite the advantages listed above, there are several risks directly related to cyber information sharing among organizations. An analysis of these risks must occur in the setting of an organizational risk management strategy and include the probability of every risk, its effects, the controls required to keep it in check, and the ways to reduce it. For example, the way to reduce the risk of legal exposure to lawsuits for revealing personal or commercial information is by means of laws and guidelines providing legal protection by the government or regulatory body. Another example is the risk of loss of organizational information assets as the result of uncontrolled sharing. That risk can be reduced by using a built-in, standardized sharing format that does not include sensitive information, as well as other checks such as instructions, regulations or legislation that will force the organization to remove personal or commercial data from the information meant to be shared before sending it.

Business Opportunities

The development of cyberspace threats and changes in organizational attitudes towards sharing are a business opportunity for the manufacturers of technological solutions, integration companies and service providers that can leverage their base of products, knowledge and services to create added value in the context of the sharing challenge.

One example relates to the challenges posed by innovative attack technologies, such as the Advanced Persistent Threat (known as APT),[20] or taking advantage of undetected or untreated security breaches. Both of these attack mechanisms reduce the effectiveness of the traditional security measures[21] but can, to a certain extent, be addressed by an inter-organizational security sharing service. Such sharing could facilitate the identification of an anomaly in the cloud and comparison with organizational events not only with regard to its conduct within the organization but also to that within similar organizations, thus enhancing the identification mechanism and reducing the risk that harmless traffic will accidentally be identified as malicious (known as "false positive"). In addition, after the identification of an attack or attacker in a given organization, the components or the inoculation can be distributed to other organizations and thereby prevent similar attacks.

Several security systems manufacturers provide solutions to cyber information sharing based on a decentralized infrastructure of information gathering, using a system of probes, which may at times also serve as honeypot traps for attackers. These are installed in organizations and end clients or at central internet nodes belonging to the manufacturer. This infrastructure gathers information on attacks and attackers in real time, in cross-referencing geographical location and attack, and distributes it as a service to the organizations involved in sharing. The system serves as a share-based database on attackers and/or attacks in the cloud and may sometimes include a component that filters and blocks potential attacks on the basis of the information being dynamically updated.

In the case of cloud-based communications and storage service providers, sharing is an opportunity to reduce the rate of client dropout by means of providing the added value of another layer of protection.[22] The nature of a shared cloud allows the provider to improve the security policy for all the other hosted organizations in order to prevent its recurrence after identifying and stopping an attack in one organization.

Another business opportunity directly related to sharing initiatives is the construction of a solution for gathering, analyzing and distributing cyber information at the national or market sector levels. Several integration companies in the world have a comprehensive solution for creating a situation assessment, analyzing events, distributing inoculations, training simulators, and other components, at the scale of military and large public systems. Moreover, there are solution manufacturers in the field of monitoring and in-depth analysis of traffic (deep packet inspection), allowing telecommunication service providers to selectively share information with the legal authorities so that the latter may listen in on telephone and internet networks for the sake of identifying threats. Some of these companies also provide the solution component responsible for information analysis based on smart logic, containing analysis of a tremendous amount of information gathered from various sources, study of anomalies, and correlations among the events.

One may assume that the wave of technological innovation in the world of security solutions will continue because of the need to adapt security systems to existing and emerging cyber threats. Furthermore, one may assume that the idea of sharing–taking on greater prominence in the security policies of key organizations–will continue to present business opportunities to commercial entities operating in the field.

Regulation and Privacy

There are fields in which the regulatory body and/or the law already require sharing information about cyber threats and cyber events, and it would seem that this trend is on the rise given governments' need to establish a national security system to fight cybercrime and maintain transparency regarding cyber-related events in public companies and strategic market sectors, such as communications, finance and healthcare. Moreover, various regulators, such as Basel III and ISO-27032, encourage sharing information between organizations and the authorities, both by means of guidelines and by offering economic benefits and relief to participating organizations. A paper analyzing the trade-off in financial institutions between investing in information security and sharing cyber information[23] concluded that the benefits of sharing among organizations increase in correlation with their interdependency, and the more sharing there is among such institutions the smaller their investment in information security. In many market segments (such as finances and telecommunications) the links between the organizations are critical to their everyday functioning, and an attack on one organization could propagate and damage the functioning of other organizations in the same sector. Examples are financial transactions between different banks and phone calls between different service providers.

Similar organizations also share similar challenges, some of which may be unique to their sector. For example, healthcare organizations share the unique challenge of confronting cyber attacks aimed at medical equipment. Cooperation among such organizations on the gathering of intelligence or hardening procedure for such equipment will save on the investment each of the organizations has to make on its own.

Several nations have iterated their intention to establish systems for gathering cyber information, including the incorporation of government bodies and private/public bodies of national importance.[24] The essence of this move is to create a comprehensive cyber situation assessment, providing the ability to respond to attacks with highly trained personnel, and immediately disseminate inoculations or information about the attack to all subordinate organizations. As noted, the technological base for creating such a system may require legislation, and requires cyber information sharing among organizations and the establishment of a center for fusing information and applying defense mechanisms to secure organizational assets and privacy. The British government has established a sharing initiative called the Cyber Security Information Sharing Partnership (CISP) as part of its national program for coping with cyberspace challenges.[25] The partnership already includes more than 250 key organizations as well as the legal authorities, and its purpose is to improve the ability to cope with cybercrime and cyberterrorism. Since the beginning of the 21st century, the United States has instituted sharing initiatives named Information Sharing and Analysis Centers (ISAC) in sectors such as healthcare, finance and more. Most of these initiatives are owned and financed by the participating organizations, but recently they have benefitted from technological and even financial support from the US Department of Defense, thus acknowledging the government's interest. Examples of involvement include providing access to the United States Computer Emergency Readiness Team (US-CERT)[26] and establishing a master initiative designed to unite all the inter-organizational information in the United States into a single system.[27]

It is obvious that fighting cybercrime and cyberterrorism, which by their very nature cross geographical and political borders, can succeed only through technological and legal cooperation among nations. One such initiative is the program for research cooperation in the field of cyberspace initiated by NATO and the EU.[28] Another initiative is the sharing infrastructure being built at NATO, in which the information will be automated on the basis of STIX in order to allow sharing among various organizations in NATO member nations.[29] Legally, the Convention on Cybercrime (also known as the Budapest Convention) was formulated and signed with an eye to coordinate the various legislative systems of the EU member nations, improve joint investigative methods, and increase cooperation in dealing with computer crime.

A paper surveying international cooperation in protecting critical infrastructures against cyberattacks[30] reinforces the hypothesis that the chances of an information sharing system succeeding increase if the participating entities have similar interests and cultural and political outlooks. Information sharing among different entities is naturally challenging in terms of maintaining secrecy because it requires a definition of the limits on sharing and controls that can distinguish between private or intra-organizational information and information that may be shared.

Over the years, governments have received tacit cooperation, which is sometimes enforced through legislation, from infrastructure and service providers, as well as application vendors, both for the purpose of national security and for the purpose of fighting cybercrime. This phenomenon received much attention recently, especially after *The Guardian* revealed, on the basis of Edward Snowden's leaks, the US National Security Agency surveillance of computer traffic of leading US companies in the context of its PRISM program.[31] The newspaper also revealed that the NSA-equivalent British intelligence organization GCHQ, monitors the internet traffic on Britain's fiber optic network,[32] and that MI5, Britain's security service agency, intends to deploy technological measures to enable filtering key words and specific data in all information traffic in the country.[33]

The exposure of the surveillance programs in the United States raised the issue of privacy and limiting the power of the government as well as the possibility of imposing legal sanctions against the parties that share their information. So far, the United States Supreme Court has rejected lawsuits against local telecom giants and confirmed the legality of submitting information regarding Internet and telephone use to legal and intelligence agencies.[34] Still, the possibility of lawsuits against an organization that shares information is an obstacle to sharing that the government would like to remove.

Since the end of 2011, legislation on cyber information sharing has been advanced.[35] The purpose of the proposed law is to allow private and public companies, in the context of cyberwar, to share information in real time with the government, law enforcement and intelligence agencies without risking lawsuits for violating secrecy or privacy. The bill passed in the House of Representatives, went through a round of adjustments in the Intelligence Affairs Committee,[36] and is still in the process of legislation in the Senate. Its opponents claim that it violates the Fourth Amendment to the Constitution,[37] which defines parameters for search and seizure of citizens' personal information, such as warrants or reasonable grounds. According to opponents of the bill, the new legislation would allow intelligence agencies to receive personal or commercial information from infrastructure and content providers without the checks delineated in the Fourth Amendment. Groups dealing with the problems inherent in the bill[38] are trying to enlist public support to oppose and prevent it from becoming a law, by running a campaign in the social media and on the internet in the United States.

The tension between supporters and opponents of cyber information sharing legislation is not unique to this area, but touches on the entire issue of privacy in the interface between the state and its citizens and the involvement of Big Brother. An example of a similar conflict may be found in the Smart City initiative in Britain, which includes covering cities with cameras and face recognition software.

Concluding Insights

Trends in the contemporary development of the cyber threat phenomenon include using attack methodologies focused on specific targets rather than being randomized, crossing geographical and legal borders, taking advantage of unidentified vulnerabilities, and using bits of malicious, modular code in cyberspace. The attackers maintain a flourishing, structured community with internal order and a supporting system of financing, allowing easy and rapid sharing of attack information. It seems that the realization of the community model on the defensive side and transitioning from a paradigm of isolated organizations to an information sharing initiative will lead to better results. In a broader view, one of the most significant resources coming into being in the 21st century is the wisdom of crowds.

One can see examples of crowdsourcing in many fields and, in this sense, cyberspace is no exception.

The transition to models of sharing is supported by the congruence of interests of most of the market forces involved, including regulatory bodies, governments, law and intelligence agencies, solution manufacturers and service providers, and even the organizations themselves. The value of sharing with external elements is, among other things, a product of the isolated organization's inability to fight its cyberwars on its own. Sharing contributes not only to significantly strengthening the security system and its survivability, but also to the organization's business success as it saves on investment, is granted preferential treatment by the regulatory bodies, and more.

The architecture of the solution and developing standards will, in the future, make it possible to create a technological structure connecting organizations while keeping their assets separate. They will also support links among separate sharing systems that can connect one another into a hierarchic structure of information, such as sharing within a market segment that will interface into cooperation at the national level.

Some of the success of the entire standardization process depends on support from the market forces. In this case, it seems that elements in the US administration, especially the Department of Defense, are determined to promote the process. Nonetheless, we still don't see effective large-scale information sharing because of the many challenges, not necessarily technological, and at times because of the conservative approach of organizational decision makers.

As the field comes of age, we may first expect to see sharing among similar organizations in the same sector and, later on, the implementation of information sharing on a larger scale. Shared interests, similar organizational cultures, and inter-organizational dependencies increase the chances of success of the initiative and reduce its risks.

Two of the prominent obstacles to sharing are the organizations' concern that if systems are linked, sensitive internal information may be exposed to the competition, and that they may receive incorrect cyber information because of the poisoning of a shared database, which might damage service provision. One can significantly reduce the risks inherent in both by technological means and standardized processes and protocols implemented both on premise and in the central sharing entity.

The greater challenge is faced by organizations whose business is essentially linked to cyberspace, such as security solutions, software products and services manufacturers, and the large project and integration bodies in the field. The question remains: is it possible to formulate a worthwhile working model among these manufacturers so that they will share cyber information, even though security and cyberspace are part of the field in which they compete? Such a model must include both elements of competition and of cooperation (coopetition) in a way that would provide advantages to each of the partners over time.

The disagreement between supporters and opponents of information sharing will continue. Given that, and given all the aspects of the topic discussed in this essay, the question that must be asked is this: is there a different paradigm in the world of information technology that would allow dealing with current and future cyber challenges without the need for sharing, or is there no choice but to join forces in the battle and rapidly adopt uniform standards for a sharing infrastructure? Either way, such an infrastructure must maintain a balance between individual rights and the state's ability to defend its infrastructures, assets and citizens.

Notes

1 A zero day attack exploits a security breach in the attack target's component that is unknown to the component's manufacturer or anyone else other than the attacker, or one that is known to the manufacturer but for which it has yet to distribute a patch.

2 One study conducted in the past year by the RAND Corporation analyzes the way in which cyberspace black markets are constructed and operate, surveys historical trends, and provides forecasts for the future. Researchers at the institute conducted in-depth interviews with experts who are officially and unofficially involved in these markets, including academics, security researchers, journalists, security providers, and law enforcement personnel. The report concluded that the black markets in cyberspace are a multi-billion dollar industry with solid infrastructures and a clear social and organizational structure. L. Ablon, M.C. Libicki and A.A. Golay, *Markets for Cybercrime Tools and Stolen Data*, RAND Corporation, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

3 The approach supporting compartmentalization of cyber information is described in many sources as part of an organization's preparation for a cyber event. An example is the preparation model suggested by SANS, taken

from a course dealing with the topic. E. Skoudis, ed., "Security 504: Hacker Techniques, Exploits & Incident Handling," *SANS Institute* (2006).

[4] L.A. Gordon, M.P. Loeb and W. Lucyshyn, "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting & Public Policy* 22, no. 6 (2003): 461-85.

[5] Basel III is a regulation in the field of finance that includes a chapter requiring financial organizations to share cyber information as part of their operational risks. For more information: *Basel III: A Global Regulatory Framework for more Resilient Banks and Banking Systems*, http://www.bis.org/publ/bcbs189.pdf.

[6] A standard which includes guidelines on cybersecurity, and the demand that organizations share information. "ISO/IEC 27032:2012–Information Technology–Security Techniques–Guidelines for Cybersecurity," July 16, 2012, http://www.iso.org/iso/catalogue_detail?csnumber=44375.

[7] The three fundamental elements of CIA represent the classic basic principles of cybersecurity: confidentiality–protecting the contents from being read by unauthorized personnel; integrity–protecting the contents from alteration by unauthorized personnel; and availability–keeping the information and systems available.

[8] TCG website, http://www.trustedcomputinggroup.org/.

[9] "Cyber Information-sharing Models: An Overview," MITRE, October 2012, http://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf.

[10] Information fusion is a process designed to link and cross-reference data, information and knowledge in order to find correlations for the purpose of improving the ability to locate and identify entities about which information is being gathered, and for the purpose of assessing a situation and ranking risks. In addition, an assessment of the outputs quality is made and demands are created for information sources, as an integral part of the fusion process for the sake of improving the outputs.

[11] Database poisoning using false information is liable to obstruct the organization's activity, internally or vis-à-vis outside bodies (denial of service). The advantage of an automated system of sharing is also its greatest disadvantage, and it is more prone to such poisoning than a manual sharing system because it does not include human monitoring in real time.

[12] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)," February 2014, http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf.

[13] M. Davidson, C. Schmidt, "TAXII Overview," version 1.1, January 2014, http://taxii.mitre.org/specifications/version1.1/TAXII_Overview.pdf.

[14] "CybOX–Cyber Observable eXpression–A Structured Language for Cyber Observables," 2014, http://cybox.mitre.org/.

[15] An example of a fundamental architecture of sharing relating to the issue of trust in the context of academic research is an architecture called PEI proposed by Krishnan and colleagues. It includes three required layers:

the policy layer, which sets out the goals of sharing and the articulation of objectives; the enforcement layer, which includes the basic solution architecture; and the implementation layer, which entails delving into the technological level of the details of sharing. R. Krishnan, R. Sandhu, and K. Ranganathan, *PEI Models towards Scalable, Usable and High-Assurance Information Sharing* (New York: ACM, 2007), pp. 145-50.

16 The federally-financed MITRE research institute delineates the stages and decisions that must be made as part of a process of constructing a sharing model. Those decisions include the sharing architecture, the model of trust among the participants, automation of sharing, operations and participants. V.B. Bakis, "Cyber Partnership Blueprint: An Outline," MITRE, October 2013, http://www.mitre.org/sites/default/files/publications/Bakis_Partnership_Blueprint_Outline_0.pdf; The Bipartisan Policy Center has come up with a model in which a central body serves as a clearance center for shared information of critical infrastructure institutions in the United States. "Cyber Security Task Force: Public-Private Information Sharing," Bipartisan Policy Center (BPC), July 2012, http://bipartisanpolicy.org/library/cybersecurity-task-force-public-private-information-sharing/.

17 A. Merchant-Dest, "How the Department of Defense and the Department of Homeland Security are Taking Steps toward Information Sharing," *Federal Blue Print*, March 2014, http://federalblueprint.com/latest-news/department-defense-department-homeland-security-taking-steps-toward-information-sharing/.

18 The South Korean research team's experiment proves that sharing information among different parties (zones) shortens response time to attacks and raises the level of security. V. B. Chang, D. Kim, H. Kim, J. Na, and T. Chung, "Active Security Management Based on Secure Zone Cooperation," *Future Generation Computer System* 20, no. 2 (2004): 283.

19 The Israeli Ministry for Environmental Protection, "Procedures and Guidelines on Emissions of Industrial Pollutants." http://www.sviva.gov.il/subjectsEnv/SvivaAir/Industry/Pages/Regulations.aspx.

20 APT is a collection of cyber attack tools and methods aimed at a specific target and controlled by professional hackers, and which can therefore be developed and operated in a way that makes it very difficult to identify using standard security measures.

21 These two attack technologies reduce the effectiveness of the traditional security mechanisms whose main function is to identify clear patterns of attack. They require behavior based reference in order to identify the threat and a transition from developing signature based security products to behavior based anomaly detection products. Two of the main challenges in the latter is the need to create an organizational behavioral baseline that documents the normal behavior of the organization and its computer systems in order to identify anomalies, and the risk to disruption of legitimate transactions because of false positives.

22 Also called Managed Security Service Provider (MSSP).

23 K. Hausken, "Information Sharing among Firms and Cyber Attacks," *J. Account Public Policy* 26, no. 6 (2007): 639-88.

24 An example of a nation's strategy in constructing a national cyber system may be found in a document of the Finnish government that includes visions and principles in building a cross-organizational cyber system and a list of concrete recommendations to make it happen. *Finland Cyber Security Strategy*, Secretariat of the Security Committee, 2013, http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

25 The British government's national program for confronting cyber threats. *The National Cyber Security Strategy, Our Forward Plans–December 2013*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf.

26 The US-CERT–United States Computer Emergency Readiness Team website, http://www.us-cert.gov.

27 The Information Analysis and Sharing Centers website– the National Councils of ISACs, http://www.isaccouncil.org/memberisacs.html.

28 *The Multinational Cyber Defense Capability Development (MNCD2) Program*, http://mncd2.ncia.nato.int/Pages/default.aspx.

29 *The Cyber Security Data Exchange and Collaboration Infrastructure (CDXI*); L. Dandurand, *Cyber Security Information Exchange*, http://www.rsaconference.com/writable/presentations/file_upload/sect-t08-cyber-security-information-exchange.pdf.

30 L. Tabanski, "International Cooperation in Critical Infrastructure Protection against Cyber Threats," *Atlantic Voices* 2, no. 9 (2012), http://sectech.tau.ac.il/node/114.

31 Electronic surveillance program carried out by the NSA, starting in 2007, to gather information for the purpose of intelligence from infrastructure, software and contents providers (Google, Yahoo, Microsoft, Apple, Skype, AOL). This activity was revealed through Edward Snowden's leaks to *The Guardian* in 2013.

32 E. MacAskill, J. Borger, N. Hopkins, N. Davies, and J. Ball, "How does GCHQ's Internet Surveillance Work?" *The Guardian*, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

33 Monitoring technology allowing the filtering of key words in internet traffic is called "deep packet inspection."

34 The United States Supreme Court rejected a lawsuit against the giant telecom companies Verizon, Sprint and AT&T, and confirmed the legality of transferring information from emails and phone conversation to the NSA. B. Kendall, "High Court Lets Telecom Firms Wiretap Immunity Stand," *Wall Street Journal*, October 9, 2012,

http://online.wsj.com/news/articles/SB100008723963904440242045780463128965 01562.

35 The Permanent Select Committee on Intelligence, 2013, *Cyber Intelligence Sharing and Protection Act of 2013*, http://intelligence.house.gov/bill/cyber-intelligence-sharing-and-protection-act-2013.

36 The modified bill after the changes is called: "Cybersecurity Information Sharing Act of 2014." Continuous updating on the status of the legislation may be found at the Library of Congress, http://thomas.loc.gov/home/thomas.php.

37 The Fourth Amendment reads as follows: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

38 Two of the institutions active on the topic are the Electronic Frontier Foundation (EFF) and Fight for the Future. Both are running a campaign called "CISPA Is Back" to gather citizens' signatures on a petition against the legislation. http://www.cispaisback.org.