Center for Cyber Security and
International Relations Studies

Co-operation and exchange of information on cyber threats being an effective measure for providing security to the organization.

Jaroslaw Sordyl

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Research Analysis

April 2020

Center for Cyber Security and International Relations Studies (CCSIRS)

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

Co-operation and exchange of information on cyber threats being an effective measure for providing security to the organization.

Jaroslaw Sordyl

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

April 2020

About the author

Jaroslaw Sordyl IT/OT cybersecurity expert with over 24 years of experience with specialization in Industrial Control Systems, risk and resilience in Industry, incident management and Information Security Management System. Trainer and lecturer cooperate with academia, universities and training centers delivers lectures concerning all aspects of ICS, information security, incident management, risk management (ISO/IEC 27005), ISMS (ISO/IEC 27001), BCM (ISO/IEC 22301), cyber threats and investigations on cybercrimes.

Former Cybersecurity Director at top 5 companies from oil and energy sector in Poland, responsible for all aspects of industrial cybersecurity. Former Head of Incident Response Team in the one of the biggest energy company in Poland. Member of the management board at EE-ISAC (European Energy – Information Sharing Analysis Center).

Holder of many of IT certifications: CISSO, CDFE, CPTE, ISO/IEC 27001 - Lead Auditor, CDRE, Lead PenTest Professional.

Co-operation and exchange of information on cyber threats being an effective measure for providing security to the organization

For the last few years, cyber security has been the matter of concern for most of organizations, independent of their size. Statistics point to alarming yearly increase in threats on the part of groups or even individual „hackers" attacking our systems. During the meeting in Davos, the participants of the World Economic Forum highlighted again, how harmful the effects of the cybercriminals' activity could be, whose attacks lead to disturbance of functioning of both individual PCs and the whole computer systems belonging to cities or global companies.

From the very beginning of the occurrence of events and incidents related to cyber threats, persons responsible for cyber security, companies' directors and CEOs consider the problem and look for some solutions. Cyber security is not a product and it can't be bought. It is a complex process, consisting of people – users, technology, including that being a part of a system cyber security, and procedures, which not only maintain functioning of the so-called business, but they also make a part of overall security. While analyzing many cases of cyberattacks, it might seem, that such solutions are sufficient for providing cyber security, as well as monitoring and reacting to incidents. How could such solutions be facilitated? Is it worth to focus on „preventive," proactive activities, i.e. such activities, that could prevent from cyberattacks and „actively" effect on decisions made on protective measures, allowing the person responsible for the cybersecurity system, e.g. CISO (Chief Information Security Officer) /CCO (Chief Cybersecurity Officer) for a quick modification of protective measures and elimination of vulnerabilities, weak points in the organization's system and avoiding of serious problems. An important element of proactive functioning is the co-operation between organizations and companies, in which teams or specific individuals can exchange information and data on potential threats, weak points and vulnerabilities of the system, which could be used by hackers or directly related to their activity. Many "good practices" and international standards point to the co- operation and exchange of information as the necessary elements of cyber security management. Both standard ISO/IEC 27001[1] and NIST 800-5[2], among others in management of incidents, emphasize the importance of information transfer in order to take up urgent activities aiming at minimizing of the negative event or preventing from its escalation. But it is not only about the standards which prove, that such an approach works in everyday work. NIS[3] Directive concerning measures for a high common level of security of network and information systems across the EU also obliges the membership countries to begin co-operation involving, but not limited to national CERT's level (Computer Emergency React Teams) and the exchange of information on threats. Operators of key services in individual sectors of economy, transportation, and energy can also develop their teams responsible for the co-operation and exchange of information. The most important purpose? To develop one common „front", to co-operate for elimination of threats and to counteract spreading of cyberattacks and threats related to them, such as: ransomware and viruses. That is one of the purposes of the implemented law on the National Cybersecurity System[4], which is the facto an incorporation

[1] https://www.iso.org/standard/54534.html.

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublicati ons/NIST.SP.800-53r4.pdf.

[3] Directive of the European Parliament and of the Council (EU) 2016/1148 dated 6th of July, 2016.

[4] Journal of Laws Dz.U. 2018 item 1560 – Law dated 5th of July, 2018 on the national cyber security system.

of the provisions of NIS Directive. As a part of the national cybersecurity system, several institutions and agencies from various levels were specified, which shall take responsibility for in-country management of that issue. The key issue for their effective activity is the co-operation and exchange of information, including critical events. Each key operator is responsible for notification and providing information on such a critical event without undue delay, but not later, than within 24 hours. Does such an action have any sense and what is it for? As an example of the correct approach to exchanging of information on the incident and method of further sharing of such an information, we might cite the case of Norsk Hydro, one of the biggest manufacturers of aluminum in the world. At night 18th /19th of March, 2019 the company became the victim of a cyberattack related to ransomware[5]. Immediately after the attack, employees were informed, that they shall not use the company's IT equipment and not log in the office network. The relevant services, including Norwegian CERT were notified of the event, so were the co-operating companies. What was the meaning of such a procedure? Providing information on events taking place in an organization offered a clear picture to its employees about the current condition of security. Is there any risk, may they work and if not, why? What should they do? All replies to those questions shall be provided directly after the incident has been identified and activities taken up shall be based on specific procedures, which shall be followed in such an event in the organization. The example of Norsk Hydro proved, that the exchange of information and co-operation really worked in this exceptional company's event, and communication on the whole event was

[5] Ransomware – malware, which blocks access to files/data by encrypting them on the victim's equipment. Unblocking takes place by filling up the correct combination of a decrypting key, which is provided by the attacker (but not always) after a ransom is paid.

unprecedented, in comparison to other events of that type. Not everyone knows, that such an information transmitted externally is analyzed automatically by the relevant cyber security teams in each organization, in which such teams are functioning. They check an attack vector, i.e. a method in which attacking cybercriminals got access to the organization, which resources they used, e.g. they sent an email with malicious attachment to one of the employees. Such an information equals to automatic recommendations in organizations: which things shall be paid attention to, if the access to some specific website should be blocked or if emails coming from a specific email address shall be blocked on the server. If this information had not been shared and published, the effectiveness of such an attack made by the same "hackers" could be the same at all times. Being unaware of what happens, everybody would be equally susceptible to it. Is it worth to get prepared for such an attack? Do the potential losses resulting from the attack e.g. image losses are worth of not sharing information with the others? It seems, that it's worth to counteract in each of the cases, especially, if we don't now the effects of a potential cyberattack, and who will suffer the most in result of it.

The next, very good example for the co- operation and sharing information is a network of organizations and institutions gathered around ISAC[6].

ISAC – Information Sharing and Analysis Center was developed in result of terrorist attacks in the USA in the 90-ties of the last century, at the order of the President, who required an Action and Co-Operation Plan aiming at protection of critical infrastructure in future. Most often, this formula is based on public and private partnership, although other co-operation configurations may exist, as well, where

[6] https://www.eisac.com, last access on April 2nd 2020.

co- operating organizations and companies focus on exchanging of information on threats. Moreover, they assist each other with an expert knowledge and they work out and provide analyses on thematic areas specified by the partners. One of the most popular co-operation centers in the sector of energy in the USA is E-ISAC, Energy-ISAC, gathering most of the companies in the sector, as well as public administration and law enforcement authorities. This vigorous organization delivers knowledge on safety, cybersecurity, and it also supports other organizations during incidents. In Europe, the equivalent of E-ISAC is European Energy - ISAC[7], which aims at offering the relevant support to organizations and companies in power generation sector by providing information on threats through MISP[8] - Malware Information Sharing Platform, and also by organizing training sessions for end-users. E-ISAC, EE-ISAC and their Japan equivalent JP-ISAC concluded an agreement for co-operation, which was not without significance for the intensification of the effect of the exchange of information between ISAC's from the same sector – power generation. The agreement concluded in 2018 in Las Vegas, the USA, pointed to sharing information between organizations as being crucial for the successful functioning of the agreement, while in turn, these organizations supported individual information exchange systems of each ISAC. In addition, each of the organizations may initiate projects or co-operate and support initiatives resulting in improvement and efficiency of security systems of all parties of the agreement.

Each sector of economy in each country may create its own co-operation centers, it is not complicated, remaining centers are always ready to assist their "colleagues". The questions of purely practical

[7] https://www.ee-isac.eu, last access on April 2nd 2020.

[8] https://www.misp-project.org, last access on April 2nd 2020.

co-operation – the exchange of information – are much more problematic. Especially in such areas, as safety and cybersecurity, there is a belief and practice, that ‘sensitive’ information shall not be distributed out of the company’s premises. On one part, it is justified, but ICAS centers are usually organized based on agreed-on statutes and regulations, including protection of the exchange of information and clauses referring to potential breaches of such agreements. However, in spite of such solutions, there are still some “communication” barriers.

Looking at the present system of information exchange and co-operation in various countries, sectors or organizations, it is difficult not to observe, that we are facing various systems which organize this exchange and co- operation, and also various formal and non-formal rules. Regardless of whether it is a form of co-operation based on legal regulations or good practices – standards or voluntary association within an organization, such as ISAC, there is one aim – the exchange of information and development of conditions for counteracting. This “prevention”, anticipation of actions of „hackers” or organized groups, trying to break our security in an organization makes one of the key targets of this co- operation.

Which model is more efficient and worth joining or applying? Probably everyone can find some arguments in favor of one or another solution, but one should recall the most important thing, regardless of the chosen model of co-operation, the exchange of information at such dynamic changes in threats on the part of cybercriminals is, at the time being, the only and one of the most effective (or even the most effective) measures in hands of “the defenders.” Things, which we exchange and how we do it are significant, and each person who shall try and check at least once how it all works, will become convinced.

In the next updates of legal regulations, the subject of co-operation shall definitely become one of the most important elements of the organization of cyber security, even by the virtue of the organization of functioning of companies. Not only are they concentrated in a specific sector, but they also co-operate with third parties in a form of deliveries or collection of goods. How the problem of potential threats during the exchange of information, e.g. orders and commercial correspondence, shall be dealt with then? We can't close the company and state, that we are not co-operating, as without it, it would be impossible to continue our business. Safety of deliveries, the so-called „supply/delivery chain" must be covered by the whole system of co-operation of the exchange of information, because it is in the interest of all participants of the system.

Probably, there are more such areas, for which the co-operation and exchange of information are crucial, it is worth to pay attention to that and take up every initiative that shall finally result in more efficient protection of the organization.

Center for Cyber Security and International Relations Studies (CCSIRS)

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html