LEX LOCALIS

Activities for Cybersecurity as a Mission of Information Sharing and Analysis Centres

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ

Abstract Today's environment of cybersecurity threats poses a challenge that has never been greater before, and the need to ensure cybersecurity is particularly notable amidst the COVID-19 pandemic. The increase in the number of sophisticated cyber attacks directed against governments and enterprises – in particular, public entities – has revealed the need to build cybersecurity strategies practically in every sphere of our lives. Organisations therefore need to protect themselves against cyber attacks in which the collected information is at the same time their primary source and target. Due to the increasing need for ensuring cybersecurity, the benefits that can be derived from joint actions seem obvious. However, the key element of such coordinated measures is information sharing and prompt response. Organisations operate better in a situation where threats are identified and described, if they are better informed about the perpetrators and the methods of attacks. Information Sharing and Analysis Centres are one of several tools used with a view to ensuring cybersecurity.

Keywords: • cybersecurity • cyber attack • threat • information

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Dr. Habil., University Professor, Head of the Media Law, War Studies University, Faculty of National Security, Intellectual Property and New Technology Department Institute of Law, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, e-mail: k.jentkiewicz@akademia.mil.pl, ORCID: 0000-0003-0188-5704.

https://doi.org/10.4335/2022.1.4 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

By design, the Information Sharing and Analysis Centre (ISAC) is a trusted sectoral unit which may provide 24/7 secure operational capability and which sets out the requirements concerning coordination, information sharing and analyses in the event of cybernetic incidents, threats and vulnerabilities in ICT networks. On the one hand, ISAC may serve as a sectoral resource, thanks to which it is possible to collect key information about incidents and issues related to cybersecurity in a given industry, and to identify, communicate, and analyse the potential outcomes of such problems for a given sector. On the other hand, the establishment of ISAC does not necessarily need to entail measures taken only in a given sector. Coordination may refer to joint undertakings or to the achievement of joint objectives related to the need to ensure system-based protection. The common denominator for the activities of partners in the sphere of cybersecurity is often the strategic nature of their services, constituting a crucial point on the map of a critical state infrastructure.

ISAC's mission is first and foremost to increase the sectoral capacity to undertake measures for cybersecurity, respond to threats in the cyberspace, search for vulnerabilities and mitigate the effects of incidents by providing a centralised organisation dealing with the monitoring and dissemination of information. The primary objective is to obtain accurate, useful and relevant critical information whose scope is as useful for cybersecurity as possible. A secondary, but equally important, objective is to maintain the confidentiality of such information, which is deemed significant for cybersecurity by ISAC members. Accordingly, it can be said the ISAC itself constitutes a platform where members can exchange information within their sector, with other organisations, and the government, which means that it is a communication tool and serves as the main communication channel in the sphere of security for a given industry. It ensures the analysis of proper threats, vulnerabilities and incidents. Moreover, it provides access to alerts concerning threats, warnings, guidance, notices and vulnerability analyses to ISAC members.

2 ISACs and critical infrastructure (CI) – the American organisation model

In 1998 B. Clinton's administration issued Presidential Decision Directive 63 (PDD-63) in which the U.S. Government requested that each critical infrastructure sector (in the USA, critical infrastructure sectors include: the chemical sector, commercial facilities sector, critical manufacturing, dams, defence industrial base sector, emergency services, energy sector, financial services, food and agriculture, government facilities, healthcare & public health, Information Technology sector, nuclear reactors, materials and waste sector, transportation systems, and the water and wastewater systems sector) identify sector-specific information to assess a given sector's vulnerability to cyber-attacks or physical attacks, recommend a plan to eliminate significant vulnerabilities, propose a system for identifying and preventing attempted major attacks, and develop a plan for alerting, containing and rebuffing an attack in progress and reconstitute minimum essential capabilities in the aftermath of an attack. In response to these needs, the owners and operators of key resources of critical infrastructure established ISACs. In 2003, Homeland Security Presidential Directive (HSPD-7) expanded the scope of PDD-63, ordering that the public and private sectors share information about physical and cyber threats, and vulnerabilities with a view to ensuring the protection of critical infrastructure in the USA. Ten years later, in 2013, Presidential Policy Directive 21 (PPD-21) updated the federal approach to critical infrastructure security and resilience by establishing closer links between physical security and cyber security and by strengthening critical infrastructure resilience with three strategic imperatives: 1) to refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience; 2) enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and 3) implement an integration and analysis function to support planning and operations decisions regarding critical infrastructure.

On the same day, President B. Obama issued Executive Order (EO) No. 13636. The document was aimed at improving critical infrastructure cybersecurity by streamlining information sharing between governmental agencies and between the public and the private sector entities, thus increasing the volume, timeliness and quality of cyber threat information. ISACs were established for specific sectors to ensure national security in the protection of critical infrastructure.

ISACs in the USA are used in multiple CI sectors in order to join the efforts of industries and the government, and to ensure measures for quick access to persons affected by cyber-attacks. A lot of these are “inter-sectoral” ISACs (e.g. communications, IT sectors, inter-state ISACs, etc.) that bring together owners of CI or service providers, and operators representing numerous sectors. The key ISACs in the USA include: 1) Financial Services ISAC: The centre has over 4,600 members and 39 partner associations, with an outreach to 99 percent of all banks and credit unions, and covers 85 percent of the securities sector and nearly 50 percent of all insurance firms; 2) Information Technology ISAC: through its members, it reaches 90 percent of all PCs and operational systems, covers 85 percent of all data bases, 85 percent of all routers, and 65 percent of all software safeguards; 3) Communications ISAC: the DHS National Coordinating Center for Communications cooperates with the private sector, including ISACs, in order to ensure 24/7 operational support. Its members include communications equipment and software providers, and it covers 95 percent of all cable lines of communications service providers, 90 percent of all wireless communications service providers, including satellite communications services, and 90 percent of the backbone network of online service providers; 4) Water ISAC: currently provides information about the security of water supply and wastewater companies, and serves over 65 percent of the American population; 5) Multi-State ISAC: covers all 50 states, the District of Columbia, four USA territories and numerous local government authorities. Moreover, MS-ISAC is continuously extending its operations, and they currently cover all 39,000 municipalities; 6) transport was identified as one of the key sectors, with four existing transport ISACs: a) the Surface Transportation ISAC: In 2002, at the request of the Secretary of Transport, the Association for American Railroads established ST-ISAC. ST-ISAC serves 95 percent of the total North American rail infrastructure; b) Over the Road Bus ISAC: supported by ST-ISAC, the American Bus Association initiated the operations of the OTRB ISAC in 2013. ABA provides security alerts and password-protected information in the relevant section of their website; c) Public Transportation ISAC (PT-ISAC): The American Public Transportation Association was appointed by the U.S. Department of Transportation as the sector coordinator for the public transport industry in the United States. To this end, APTA established PT-ISAC. APTA members provide services to over 90 percent of all public transport users in the USA and Canada; d) Maritime ISAC: This ISAC is a non-profit organisation sponsored and managed by the Maritime Security Council. The Maritime ISAC cooperates with the U.S. and international maritime shipping, seaport and government regulatory oversight communities. It deals with collecting and analysing proprietary data (e.g., stowaway rates and locations, drug seizures overseas, terrorist threats etc.), which it then disseminates to participating industry and government constituents; 7) Retail ISAC: The Retail Cyber Intelligence Sharing Center acts as a platform for retailers where they can exchange information on threats and leading practices, at the same time improving the security of retail networks and protecting consumer data. The analysts of the Retail ISAC process and collect real-time information on cyber threats (including new types of malware, the operations of underground criminal forums or potential software vulnerabilities). It also provides anonymised information to the federal government and law enforcement bodies, such as the DHS, Secret Service or the Federal Bureau of Investigation (Goodwin, Nicholas, 2015).

3 The cooperation of ISACs with other entities

The analysis of American ISACs reveals close links between government agencies and ISACs in the sphere of counteracting cyber-attacks. The transportation sector is one example of this. Along with the update of the national approach to the security and resilience of critical infrastructure, 16 critical infrastructure sectors were identified, and the related sector-specific federal agencies were appointed. The Department of Transportation is responsible for providing technical support to CI owners and operators, and for facilitating access to, and exchange of, information necessary to enhance and protect transportation security. DHS manages the National Cybersecurity and Communications Integration Center, which is a centre responsible for coordinating emergency information about cyberspace and communications across the country, operating 24/7, engaging in cooperation state and local authorities, intelligence communities, law enforcement bodies and the private sector. The Operational Control and Emergency Communications Center is a centralised institution whose objectives are to ensure cybersecurity and to raise the awareness of threats in the sphere of communications, vulnerabilities, hacking, incidents, as well as mitigating and recovery measures.

In 2011 DHS launched an information sharing and cooperation programme in respect of the cyberspace in order to raise awareness within all critical infrastructure sectors through a close and timely exchange of information about cybernetic threats and direct analytical exchange. The programme covers governmental organisations, ISACs and other CI owners and operators through the development of a mechanism by which private sector partners would be able to share data directly with the government via an inter-sectoral portal. Fully integrated divisions allow a holistic approach to cybersecurity and communications issues at the operational level. The sectoral partnership model is set out in the National Infrastructure Protection Plan (NIPP). The model encourages CI owners and operators to establish Coordinating Councils which are to: 1) represent principal entry points for the government to collaborate with the sector with a view to solving problems; 2) serve as a strategic communication and coordination mechanism between owners, operators and suppliers of IC, and, as appropriate, with the government during emerging threats or response and recovery operations; 3) identify, implement and support appropriate information-sharing capabilities and mechanisms in sectors; 4) facilitate inclusive organisation and coordination of the sector's policy development regarding critical infrastructure security and resilience planning and preparedness, exercises and training, public awareness and associated implementation activities and requirements; 5) advise on the integration of federal, state local and regional planning with private sector initiatives; and 6) provide input to the government on sector R&D efforts.

Government Coordinating Councils cooperate with ISACs. Their tasks include: 1) the provision of inter-agency strategic communications and coordination at the sectoral level through partnership with DHS, Sector-Specific Agency and other supporting agencies across various levels of government; 2) participation in planning efforts related to the revision of the National Plan and the development, implementation and revision of Sectoral Plans; 3) coordination of strategic communications and discussion and resolution of issues among government entities within the sector; and 4) coordination of, and support for, the efforts to plan, implement and execute the Nation's critical infrastructure security and resilience mission.

One of the strengths of the ISAC "system" is the exchange of data and experience with other related ISACs. The National Council of ISACs (NCI) is one of several such information sharing mechanisms. Formerly known as the ISAC Council, the NCI is a group of volunteer representatives of ISACs who meet to develop trusted relationships between sectors and to address common issues. Each ISAC appoints four representatives to the Council. The mission of NCI is to increase physical security and cybersecurity of national critical infrastructure through establishing and maintaining a framework for valuable interaction between the ISACs and the government. The NCI holds monthly meetings via teleconference and quarterly on-site meetings to discuss current issues. The

NCI also sponsors the annual Critical Infrastructure Protection Congress to bring together the critical infrastructure community for networking, learning and addressing issues of concern to stakeholders. The mission of the Partnership for Critical Infrastructure Security (PCIS) is to coordinate common CI cross-sector initiatives that promote public and private efforts to help ensure secure, safe, reliable, and resilient critical infrastructure services.

Some information sharing programmes, in particular in the private sector, operate via local companies, universities and experts who discuss common threats and vulnerabilities.

In the United States, non-profit programmes, such as the Bay Area Chief Security Office Council, and the Massachusetts Advanced Cyber Security Center, are examples of regional information exchange organisations. The Federal Bureau of Investigation (FBI) also has developed the InfraGard, a regional public-private information-sharing hub.
Numerous information exchange schemes at the national level, both voluntary and mandatory, include all information-sharing participants and influence them. The inherent role of national governments in the sphere of legal regulations and security suggests the need for national information exchange programmes. In the United States, most proposals from the Congress and the executive branch are centred around participation in new national-level information sharing programmes.

Cyberthreats usually have an international reach, so information sharing participants might wish to communicate within the international agenda. For governments, such disclosure may be problematic, as the provision of sensitive or even confidential information can only occur between close allies. As a result, the efforts aimed at the establishment of international information sharing schemes in which governments participate have not been successful.

The analysis of the American ISAC model shows that mitigating cybersecurity risks increasingly depends on information sharing and cooperation between a wide range of entities, with the use of numerous diverse collaboration models, methods and instruments. The design of successful information-exchange mechanisms is not an easy endeavour, as it requires continuous engagement, trust and a clear sense of values shared by entities participating in a given project. The key element of ensuring support related to information sharing is the coordination of activities, in particular, those taken by public and private organisations. Nonetheless, it is crucial to build such information-sharing and cooperation tools among entities of substantial strategic importance for the state in the public-sector area.

4 ISAC – the European model

European ISACs differ from their American counterparts in terms of dynamics and characteristics. First of all, European ISACs build on the experience of older organisations from across the Atlantic. Secondly, European ISACs are very much distinct from the American ones, which results from cultural differences – in the USA, businesses are expected to take care of themselves, while in Europe it is expected that the state ensures cybersecurity in each sector, while the majority of key public tasks are performed in full by the public sector.

European ISACs focus on building partnerships and trust between their members. They are very industry-oriented, but there are also high expectations about governmental support – not in terms of financing, but rather in the substantive area through sharing specialist knowledge (combating cybercrime, sharing industry-relevant information). The participation of public administration increases the effectiveness of ISACs. Moreover, it proves the respect and support for market needs on the part of the public sector, in political and strategic terms (for example, such need is indicated in the Directive on security of network and information systems and in the GDPR).

The development of the ISAC ecosystem in Europe depends on the cultural conditions of individual members and the general level of trust between public and private entities – if a public-private partnership (PPP) is involved. Therefore, in countries where the trust is insufficient, it is worth starting from developing appropriate PPP structures, and then transforming them into an ISAC. This is owing to the fact that the exchange of information about incidents is very demanding, and the level of trust between participating entities is of great importance here. As key services require the establishment of this type of organisations to enhance cybersecurity, ISACs bringing together only public sector partners are also needed, if not indispensable.

It is worth noting here that international or large enterprises operating in the cybersecurity sector (in Europe) are usually not involved in ISACs. This is mainly due to the insufficient trust of ISAC members in such companies, which is based on the belief that they might use the provided information and knowledge to advance their own business. That is why the benefits that might be derived from such participation should be explored beforehand. There are three roles in an ISAC – moderator, member and partner. The moderator (leader) is an entity which defines the logistics of the group (it assumes the function of a secretariat); a member is an organisation which actively discloses or receives information; and a partner is an entity which may take part in dedicated sessions, usually aimed at providing specified information (research data) or discussing a specific topic (e.g. transposition of a directive to national law).

5 Conclusions

Cyberthreats and cyber attacks are not only a technological risk, but also a business risk. Therefore, the cybersecurity function should have sufficient independence and significance. This might help ensure the proper consideration of decisions related to risk management that are not affected by other issues and IT limitations, or overshadowed by them. If cybersecurity is part of IT, it might lack sufficient visibility and links with the actual services. Enterprises should therefore consider specific measures with a view to establishing links between services, risk partners and cybersecurity. This could be achieved through the creation of steering committees within the framework of ISACs. Such measures could also facilitate the alignment of cybersecurity measures with future business plans.

The COVID-19 pandemic has significantly disrupted the operations of institutions and their functioning worldwide. Remote work has gained popularity, and as a result, the number of videoconferences and team collaboration applications have rapidly increased. In a recent report prepared by Deloitte, it was found that many financial institutions were evaluating permanent remote work for at least part of their workforce. Indeed, based on conversations with industry leaders, some companies are considering remote work for 30% or more of their employees on a more permanent basis. Cybersecurity organisations will need to quickly adapt to this new operating environment by implementing enhanced controls and endpoint protection technologies so as to exert greater control over end-user devices. Companies should, hence, consider increasing training and awareness activities, focusing on remote etiquette for work-from-home environments. Such experience should be the subject of information exchange as part of ISACs (Bernard, Nicholson, 2020).

References:

Bernard, J. & Nicholson, M. (2020) *Reshaping the cybersecurity landscape How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions*, available at: https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (March 15, 2022).

Goodwin, C. & Nicholas, J.P. (2015) *A framework for cybersecurity information sharing and risk reduction*, available at: C:/Users/48692/Downloads/Framework_for_Cybersecurity_Info_Sharing%20(1).pdf (March 15, 2022).