INFORMATION & SECURITY
An International Journal

Scenario-based Security Foresight

Edited by
Alexander Siedschlag

Procon Ltd.

Volume 29, 2013

Volume 29, Number 1

Methods & Techniques in Scenario-based Foresight

Threats, Scenarios, Roles

Volume 29, Number 2

Scenarios and Security Research Planning

The Way Ahead

I&S Monitor

Information & Security: An International Journal

López & Pastor, vol.29, 2013, 69-76 http://dx.doi.org/10.11610/isij.2905

COMPREHENSIVE APPROACH TO SECURITY RISK MANAGEMENT IN CRITICAL INFRASTRUCTURES AND SUPPLY CHAINS

David LÓPEZ and Oscar PASTOR

Abstract: The ability to assess and therefore react to risk exposure in critical infrastructures and supply chains environments greatly contributes to reaching suitable protection levels and response mechanisms. Due to the unavoidable interdependencies among those infrastructures, that allow disruptions to spread from one to another and likely cause a great impact on society's welfare state, risk management might be seen as a common and shared concern. The Comprehensive Risk Management approach tries to face this process by gathering information from a broad range of disciplines (physical and logical security, safety, environmental threats, etc.) while taking into account interdependencies of critical infrastructures and supply chains at different layers, going from critical infrastructure operators point of view, to sectoral, national and finally supranational levels. Besides, risk assessment and management processes rely on accurate and timely information to assist decision making, but this information (security holes, attacks or even disruptions suffered by an infrastructure or supply chain)—due to its sensitiveness—does not easily flow between involved or interested parties. This paper provides an analysis of this situation and suggest future fields of action, supported by conclusions drawn from the FOCUS project.

Keywords: Comprehensive security, risk management, dynamic risk assessment, DRA, DRM, critical infrastructure protection, supply chain protection.

Introduction

FOCUS ("Foresight Security Scenarios – Mapping Research to a Comprehensive Approach to Exogenous EU Roles") project defines the most plausible threat scenarios that affect the "borderline" between the EU's external and internal dimensions to security – and to derive guidance for the Union's future possible security roles and decisions to plan research in support of those roles. As a result of this project, several future fields of action and research have been identified, involving Critical Infrastructure & Supply Chain (hereinafter CI&SC) protection. Some of the relevant ones focus on the need of a comprehensive risk-driven protection of the CI&SC, as well as decision support systems able to integrate multiple sources of data, in order to get a right situational awareness. This may lead to an improvement of protection measures applied, in alignment with the CI&SC risk exposure.

Nowadays, a wide spectrum of regulations has emerged, setting security requirements to infrastructures supplying critical services to society and allocating responsibilities in their protection at several levels: operators of each infrastructure, housing countries, supranational bodies, etc. They all face the challenge to apply commensurate security measures, balancing needed investments versus the relevance of the CI&SC missions and the whole range of risks they are exposed to (natural or manmade disasters, operational errors, physical or cyber-attacks, etc.). Involvement of national agencies, authorities, or bodies from European and international levels, as well as from CI&SC operators is now starting to be achieved. Nevertheless, there still is a manifest reluctance to share relevant information about security.

This text provides an insight into these two matters—comprehensive risk management and cooperation through security information sharing—trying to show their benefits and propose steps in order to overcome the main obstacles that nowadays avert their successful adoption.

Comprehensive Security Risk Management in CI&SC

Risk Management[1] aims to help establishing priorities and focusing security resources in order to reduce risk exposure. This is done by firstly getting a sound knowledge of key factors that negatively affect the Organization’s main processes or services. Risk Management process lays on risk assessment techniques that try to identify, analyse and evaluate—through a broad range of involved variables—potential events with a measurable impact on an Organization’s objectives.

Currently, there is a significant number of risk assessment methodologies, specifically designed to meet CI&SC requirements in this field.[2] They are usually domain-oriented which means that, depending on the sector of application and the level of abstraction (asset, system, or system of systems), a given methodology approach might fit better than another.

Risk Management in CI&SC environments may be regarded from different though compatible perspectives. Following a bottom-up approach, the risk management process should:

- Be applied in every CI Operator[3] for each CI under its control. This means that private sectors should be strongly involved, providing that most CIs are privately owned.
- Be faced at nation level,[4] given that CI services usually go beyond local or regional boundaries, conforming interrelated infrastructures and extended communication or transport meshes. This can be done by means of sectoral CI clustering (i.e. energy, transport, communications, healthcare, etc.) followed by a nationwide level of risk management, taking into account all of the previously referred sectors.
- Last but not least, be applied from a supranational point of view, because it is a known fact—as several incidents already indicated—that CI&SC are highly dependent and any disruption in the CI&SC in neighboring countries might have an impact on local critical services.

Special effort is being invested in designing frameworks[5,6] at all these levels of management, to accommodate and standardize different risk management and governance processes.

Those processes and/or frameworks rely on the gathering of timely, relevant and appropriate information about risks (threats, vulnerabilities, incidents and impacts) to information systems and the safeguards or measures to mitigate and manage those

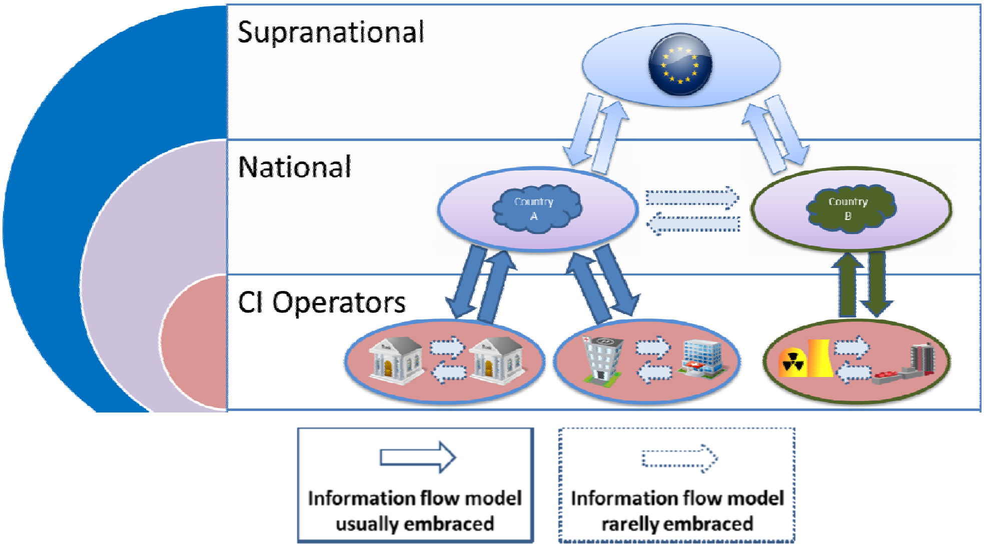
Supranational
National
CI Operators
Country A
Country B
Information flow model usually embraced
Information flow model rarelly embraced

Figure 1: Layers of Risk Management and interrelations.

risks. Unfortunately this information gathering and information exploitation are not easy due to the wide range of input variables and the yet unstandardized exchange formats to be used in order to reach effective—and automatic, whenever possible—information sharing procedures.[7]

Once a high-quality input data is supplied from all partners or stakeholders involved, depending on the level we are actually working on (CI Operators, nation-wide, or supranational), it becomes possible to get a useful outcome of the risk assessment and management processes by aggregating and analyzing the information to deliver statistical data on the risk landscape.

This ability to gather information from a broad range of disciplines (physical and logical security, safety, environmental threats, etc.) and exploit it based on a thorough analysis of interdependencies of CI&SC at different levels is seen as a comprehensive approach to security risk management. Furthermore, the capability to promptly adapt Risk Assessment to occurrence of unexpected changes, such as new threats or a breakdown in interrelated infrastructures, derives in a sound situational awareness and a more effective response. This competence to reassess risk[8] even in real-time, at the very best, is now been developed under the Dynamic Risk Assessment (DRA) and Dynamic Risk Management (DRM) concepts,[9] both having deeply relevant to the Comprehensive Risk Management approach.

Several methods to implement DRA are been considered,[10] but there still is a long way to go. One approach might be the integration of risk assessment tools with real-time security events monitoring tools, and ultimately automating response measures in line with risk management policies. This drives again the need of security data exchange standards.

Security Information Sharing

As already shown, accurate information input is crucial for valuable risk management and decision making. When analyzing risk at Operator level, information about security, or related events, certainly flows in more easily due to a sense of "being in the same boat." This information is usually directed to an identifiable security officer or alike, presumably the one accountable for risk management.

One step up, challenges grow. Sharing information about security holes, attacks or, lastly, disruptions may put Operators in a compromising situation and harm their reputation, or make them loose competitive advantage in private market environments. Unfortunately, this lack of openness also harms third CI&SC parties that might be exposed to the very same security problems and might have taken preventive measures in case of prompt notification on current risk. It is also critical to designate a national (or supranational, depending on the activity level) trustworthy central point of contact, such as CERTs, to whom affected organizations should report when things go wrong. Otherwise, security incident information may not be spread under appropriate security conditions, such as confidentiality and need-to-know principles or, even worse, organizations may be skeptical about sharing their own information.

On the other hand, collaboration between organizations, countries and EU bodies through security data compilation and information sharing would undoubtedly lead the way to a cooperative risk evaluation framework easing a coordinated, preventive, as well as reactive risk management approach. Different approaches are being proposed to foster such information sharing through cyber defense collaboration frameworks and trust relationships.

Briefly, there are four aspects of collaboration frameworks[11] that help to identify approaches for improving information sharing as follows:

- Incentives and barriers for information sharing. Aimed to identify the static structure of the information sharing network, and mainly trying to find answers of Why, Who and What of the network.
- Information value perception and collaborative risk management. Entities share information according to its perceived value, purpose, and meaning. Thus, it is critical to ensure that all entities have a common understanding of the information to be shared.
- Improving data exchange. Data models must address the information needs of the individual participants in order to provide sought-after information in a clear way.
- Automation of sharing mechanisms for technical data. An information-sharing network is likely to contain a huge amount of technical data. Automation on the selection of that data and the mechanisms to share with participants in the framework of a specific network is a key requirement to facilitate effective analysis and sharing. Moreover, the existence of an automated exchange can provide an incentive for joining the trusted network.

In the same line, the European Programme for Critical Infrastructure Protection (EPCIP) sets forth a framework aimed to support the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, a CIP information-sharing process and the identification and analysis of interdependencies.[12]

All these cooperation efforts should be assisted by agreements, focused on the promotion of information sharing aimed to an effective and timely coordination of future risk management actions. These agreements should be built on the basis of a true partnership, but a third common trusted body may be agreed and regarded as referee or collaboration enabler, i.e. delivering a secured platform for communications, identifying and trusting focal points of contact or easing relationships with authorities.

However, the ever-changing nature of incidents makes it difficult to define the scope and terms for prearranged agreements, while on-the-fly agreements may hinder effective response. In the case of cybersecurity, for example, borders and legal aspects are not sufficiently clear. Agreements will also require broad sharing of knowledge and data based on strong trust relationships, even among possible competitors in sector markets.

Conclusion

Adequate risk assessment and management processes depend on the quality and accuracy of inputs used along the process. However, fear to sensitive information disclosure makes the desirable information sharing between organizations, countries and EU bodies hard to accomplish. Trustworthiness of information sources used as inputs is also a must, otherwise assessments would suffer from unreliability.

Risk Management should be dynamic to allow adapting security measures and resources to the continuously changing environment. This can be faced by a continuous data-feeding to the risk assessment process, taking advantage of information sharing among the various stakeholders involved.

Agreements for security collaboration may be adopted both at national and supranational level, not only as information sharing platforms where security facts may be communicated with no fear of compromising, but mainly as a quick and effective way of awareness tool in order to effectively protect CI&SC against common threats and risks.

Future security research tracks pointed out as FOCUS outcomes include:

- Legal implications of cross-border agreements at different levels (countries, national agencies, companies, etc.);
- Incident response strategies and actors involved in security incident management and resolution;
- Secure communication protocols and mechanisms allowing sensitive information exchange about security and risks;
- Dynamic exploitation of information inputs in order to accurately reassess risk and ease management decision-making.

Missing expertise exists in the field of knowledge of security incident scenarios and legal matters linked to them. Moreover, more international relations expertise in the security sector will be needed in order to manage the interactions between the cross-border actors involved.

Acknowledgement: The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261633. This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained therein.

Notes:

[1] ISO/IEC 31000:2009 *Risk management – Principles and guidelines* (ISO, 2009).

[2] Georgios Giannopoulos, Roberto Filippini, and Muriel Schimmer, *Risk Assessment Methodologies for Critical Infrastructure Protection, Part I: A state of the art*, EUR 25286 EN - 2012 (Ispra, Italy: European Commission's Joint Research Centre, 2012), http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf.

[3] Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union* L345 (23 December 2008): 75-82.

[4] ENISA, *National Cyber Contingency Plans - Contents & Lifecycle* (April 2012).

[5] *Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector*, Final Report (European Commission, Directorate-General Justice, Freedom and Security, September 2009), http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf.

[6] ENISA Working Group on National Risk Management Preparedness, Consolidated Report (ENISA, April 2011), www.enisa.europa.eu/activities/risk-management/files/deliverables/WG%202010%20NRMP.

[7] David López, Oscar Pastor and Luis Javier García, "Comunicación de Eventos de Seguridad orientada al Análisis de Riesgos Dinámico," presented at the XII Spanish Meeting on Cryptology and Information Security (RECSI), San Sebastián, 4-7 September 2012.

[8] Matthew H. Henry and Yacov Y. Haimes, "A Comprehensive Network Security Risk Model for Process Control Networks," *Risk Analysis* 29:2 (2009): 223–248, http://dx.doi.org/10.1111/j.1539-6924.2008.01151.x.

[9] Néstor Ganuza, Alberto Hernández, and Daniel Benavente, *An Introductory Study to Cyber Security in NEC* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, June 2011).

[10] David López, Oscar Pastor, and Luis Javier García, "Concepto y Enfoques sobre el Análisis y la Gestión Dinámica del Riesgo en Sistemas de Información", presented at the XII Spanish Meeting on Cryptology and Information Security (RECSI), San Sebastián, 4-7 September 2012.

[11] Diego Fernández, Oscar Pastor, Sarah Brown, Emily Reid, and Christopher Spirito, "Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships," in *Proceedings of the Fourth International Conference on Cyber Conflict (CYCON)*, ed. Christian Czosseck, Rain Ottis, Katharina Ziolkowski (Tallinn: NATO CCD COE Publications, 2012), 429-445.

[12] Commission staff working document, *On the Review of the European Programme for Critical Infrastructure Protection (EPCIP)* (Brussels, June 2012).

David LÓPEZ is a senior Information Security consultant in ISDEFE as well as a PhD student in Universidad Complutense de Madrid (UCM). He obtained an MSc degree in Computer Research from School of Computer Science (UCM) in 2012, and holds CISSP, CISA and ISO27001LA certifications. He has more than 8 years of experience in information security, last three focused on critical infrastructures and Spanish Ministry of Defence facilities. He has previously worked for international companies such as IBM and Ernst & Young. His research interests are in the area of dynamic risk assessment and risk management. *E-mail:* dlcuenca@isdefe.es

Oscar PASTOR is Security Manager in ISDEFE, pursuing a PhD degree in Universidad Pontificia de Salamanca (UPS). He obtained a Research Proficiency Diploma in Software Engineering from the School of Computer Science (UPS) in 2009 and holds CISA, CGEIT, CRISC or ITIL Expert professional certifications, among others. He has more than 18 years of experience in information security, the last ten working mainly in the Spanish Ministries of Defence and Interior. As part of that cooperation, Oscar regularly attends several international security committees and cybersecurity working groups. His research interests are in the area of application of statistical methods to improve the dynamic security risk management.
E-mail: opastor@isdefe.es