Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679
ISBN 978-3-901509-83-4, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2011
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2011

MEASURES FOR CRITICAL INFRASTRUCTURE PROTECTION IN THE CZECH REPUBLIC

NECESAL, L[ubos]; LUKAS, L[udek] & JASEK, R[oman]

Abstract: *Nowadays, critical infrastructure protection is up to date, nevertheless not exactly a new issue. Despite this the EU has still not formed a consensus what measures can be used to protect critical infrastructure. This article presents five basic measures that can be used for issues of critical infrastructure protection. These measures are applicable across the critical infrastructure sectors*
Key words: *critical infrastructure protection, measures, European critical infrastructure, physical protection*

1. INTRODUCTION

The matters concerning critical infrastructure have been dealt with on European level since the beginning of the second millennium. The obligatory legislative document regulating the matters of critical infrastructure protection is a directive EU 2008/114ES "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" passed on December 8, 2008. This directive represents the first stage of the European programme for Critical Infrastructure Protection (EPCIP). Today, however, EPCIP does not regulate/define the measures that the owner/operator takes to protect European critical infrastructure (ECI). Therefore, this article presents five basic measures that can be used for critical infrastructure protection (CIP).

2. BASIC MEASURES FOR CRITICAL INFRASTRUCTURE PROTECTION

It is necessary to deal with the CIP issues as a complex system. This means that the individual measures for CIP (the ways of CIP) must be balanced, intertwined and complementary. Measures which are used (and can be used) for CIP are described in the following chapters.

2.1 Risk and crisis management

The strategy for risk and crisis management constitutes a systematic process and consists of five phases representing the necessary scope of process-based risk and crisis management in a private enterprise or a government authority. The five phases are as follows: 1. preliminary planning to establish a system of risk and crisis management; 2. risk analysis; 3. specification of preventive measures; 4. implementation of a system of crisis management; and 5. regular evaluation of phases 1 through 4.

As described in A guide of Ministry of the Interior of Federal Republic of Germany: Protecting Critical infrastructures – Risk and Crisis Management, risk and crisis management is based on a general "plan – do – check – act" (PDCA) management cycle. This allows it to be incorporated into existing management structures such as quality management, existing risk and crisis management, or process management. The term "organization" refers in this paper to private enterprises or government authorities, which operate critical infrastructures as defined above (Federal Ministry of the Interior, Federal Republic of Germany, 2006).

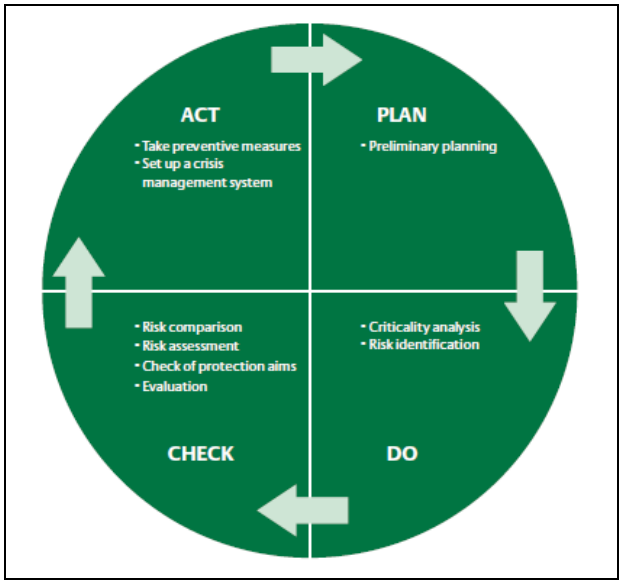

Fig. 1. The process of risk and crisis management based on PDCA (Federal Ministry of the Interior, Federal Republic of Germany, 2006)

2.2 Physical protection

Physical protection in the area of CI is secured by companies in the commercial security industry (CSI). In CSI, the physical protection of any object (building, appliance, object etc.) is achieved by combining and intertwining three basic elements: physical protection systems, response team/activity and regime protection.

1) Physical protection systems – is divided into two basic areas: mechanical barrier systems (safety locks, grilles, toughened laminated glass, safety deposit boxes etc.) and technical protection systems (Intruder and/or Hold-up alarm system; Fire alarm system etc.).
2) Response team/activity – can be carried out by own resources, security, private security service employees or by the police or army. This type of protection is expensive but very active and effective. The core is a response of a human element to impulses related to danger/security disruption/object protection such as: breaking in, technological breakdown etc.
3) Regime protection/measure – consists of a compilation of administrative and organization measures for securing protected interests and values. Generally considered the important are for example: input and output mode of persons and means of transport; mode of the employee's movement in the object; material and expedition mode.

2.3 Business continuity planning

Modernly-run organizations pay still more attention to Business continuity planning (BCP). BCP may be defined as a compilation of activities focused on decreasing the risk of collision emergence and restricting impacts on critical company

processes. It is important to realize that the continuity planning is not only a plan of a response to a critical event but also includes an important precautionary aspect. One of the main outputs from this process is Business Continuity Plan. Good quality of the continuity plans is capable of minimizing the consequences of exceptional events and at the same time they enable and accelerate the actuation of operation into a standard condition.

Good quality of the continuity plans should be a strategic aim of any organization – from big multinational organizations to small or middle businesses. Although the measure of employing specific technologies will be different in different types of organizations, it is necessary to keep the main principles of a life cycle of continuity management when designing the continuity plans. Among them there are namely a good quality analysis, testing and regular maintenance. All individual measures must be intertwined but with BCP and Risk and crisis management it applies doubly.

2.4 IT security

Dealing with IT security is a cross-cutting discipline that impacts all parts of information system. The aim of the solution is to determine rules and to subsequently ensure their observance, eventually enforce them. The reason for a proactive approach to the IT security is namely the fact that the expenses spent for precaution of security incidents are significantly lower than expenses related to eliminating their impacts.

The main elements/parts of IT security are intertwined with other measures for critical infrastructure protection. Therefore it may seem that the individual elements/parts of IT security repeat in other measures. But even that is an incorrect understanding of this problem. As it has been mentioned before, the measures for critical infrastructure protection are based on a complex approach to security. That means that there is created for example one security policy within the company which, however, includes all measures from Risk and crisis management to Physical protection. The main elements/parts of the IT security are: security policy; management of a physical access; folder services; authentization and authorization; security supervision and management system; invasion checking; antivirus protection; protection for the web's perimeter; data encryption; protecting mobile devices etc.

2.5 Personal and administrative security

In this area which observes the "life cycle of an employee", the security measures can be divided into those that are made before the employment relation emergence, during the employment relation and after the employment relation's termination or alternation.

The basis of personal and administrative security is determination and subsequent documentation of security roles and responsibilities according to the requirements of the company's security policy. In order to ensure an adequate level of security, it is necessary to carry out inspections with the new employees. That includes simple techniques such as identity verification according to documents, verification of education or training documents, etc. A higher level can be carried out by a personal profile analysis, reference verifying or business register check or insolvency register. The highest form can be done by proving integrity on the basis of the extract from the crime register or other special methods. The last stage of accepting an employee is negotiating exact conditions for work, which should also include a specification of an employee's responsibilities and duties in regard to maintaining security.

For the development of personal security during the employees' activity in an organization, three safety measures are important:

1) Senior employees' responsibility – their motivation to follow safety rules.
2) Broadening the security consciousness – the aim is to project the rules into an actual behavior of all employees.
3) Disciplinary proceeding – the aim is to discipline and draw attention to detected misconduct.

The last stage of the employee's stay in the organization is the termination of his/her employment relation. In relation to the leaving employee it is important to draw attention to the fact that his obligation of reticence continues even after his employment relation termination. Another measure is returning of all borrowed devices. The basic tasks for employees involved in the information and communication technologies are locking and deleting access accounts and closing all access routes into the organization for the leaving employee. That also includes the area of physical protection.

3. CONCLUSION

This article presented measures that are usable for critical infrastructure protection and serve to increase the security of critical infrastructure across sectors. In practice, we meet with other more specific measures by the individual owners/ operators of critical infrastructure. These are beyond the scope of this article and are different for each sector of critical infrastructure. The article presented five measures (risk and crisis management, physical protection, Business continuity planning, IT security, personal security and administrative) that are applicable across different critical infrastructure sectors. These measures are commonly used for increasing security of companies, enterprises, government organizations as well as for the critical infrastructure protection. However, for providing a similar level of critical infrastructure protection, it is necessary to define the minimum requirements that owners/operators of ECI apply in terms of these measures. These minimum requirements will be obviously different depending on sector and the importance of the element of critical infrastructure.

4. ACKNOWLEDGEMENTS

This paper was supported by the Ministry of Interior of the Czech Republic under the Research Plan No. VG20112014067 and by the Ministry of Education, Youth and Sports of the Czech Republic under the Research Plan No. MSM 7088352102 and by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

5. REFERENCES

Federal Ministry of the Interior, Federal Republic of Germany (2006). Protecting Critical Infrastructures – Risk and Crisis Management, *Available from:* http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.html?nn=106228, *Accessed on: 2011-05-28*

Doucek, P.; Novak, L. & Svata, V. (2008). *Rizeni bezpecnosti informaci*, PB tisk Pribram, ISBN 978-80-86946-88-7, Pribram

Lukas, L.; Hromada, M. (2011). Management of Protection of Czech Republic Critical Infrastructure Elements, *ACMOS'11 Proceedings of the 13th WSEAS international conference on Automatic control, modelling & simulation*, Recent Rechearches in Automatic Control, Lanzarote, Canary Islands, Spain, ISBN 978-1-61804-004-6, pp. 306-309

The Council of the EU (2008). Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *The Official Journal of the EU*, December 2008