International Journal of Economics, Commerce and Management
United Kingdom Vol. III, Issue 5, May 2015
http://ijecm.co.uk/ ISSN 2348 0386

THE NEED FOR ESTABLISHMENT OF PROFESSION "DESIGNER OF INTEGRATED SECURITY MANAGEMENT SYSTEM"

Kiril Stoichev
Institute of Metal Science, Equipment and Technologies with Hydroaerodynamics Centre,
Bulgarian Academy of Sciences, Sofia, Bulgaria
kstoichev@ims.bas.bg

Abstract

There are different methodologies and schools for the training of specialists who work or want to work in the field of security and protection of critical infrastructure. However, they all trained in one or another aspect of security and protection in the field of physical and IT security, but not in terms of design, construction, operation and improvement of integrated security systems, in terms of organizational, technical and procedural aspects. Namely thematic areas and training purposes in respect of the management and implementation of requirements for such systems is the basis of the content of this article. The main objective was to formulate a framework of requirements for the training of designers of integrated security systems.

Keywords: integrated model for security and protection, integrated security management system, professional code, critical infrastructure, integrated training

INTRODUCTION

In a series of papers presented and further developed the idea to build a security system that integrates all known as the professional audience elements and subsystems of the management system of the organization first, directly related to solving security issues, and those who indirectly affect the risk of realization of potential terrorist attacks. In one case, formulated the idea of an integrated model for security and critical infrastructure protection (Stoichev K., 2014, 1), and in the other, creating layers of security of critical infrastructure upon which to build an integrated system of security and protection (Stoichev K., 2014, 2; Stoichev K., 2015).

Both ideas are two sides of the same "coin". In confirmation of this is formulated definition of system security and protection - "The system for security and protection is a set of components operating in a single security concept, purposefully managed in a common informational environment to ensure processes, aimed early detection of threats and preventive response to prevent adverse effects" (Yachev R. 2013). In the first case the integrated model includes three main modules (Vitanov L., 2013):

- Organizational part - analysis, evaluations, policies, strategies, plans;
- Technical part; and
- Procedures for the implementation of policies, strategies and plans.

In the second, were presented levels of security for critical infrastructure, which could be defined and can be in the base of the development of an Integrated Security Management System (ISMS). The levels are as follows:

- 1^{-st} level - Risk Assessment and Internal Security;
- 2^{-nd} level - Risk Assessment, Internal Security and External Security;
- 3^{-rd} level - Risk Assessment, Internal Security, External Security, Quality Assurance and Safety;
- 4^{-th} level - Risk Assessment, Internal Security, External Security, Quality Assurance and Safety, Information Security, Human Resources and Financial Security;
- 5^{-th} level - Risk Assessment, Internal Security, External Security, Quality Assurance and Safety, Information Security, Human Resources, Financial Security, Environmental Security and Social Corporate Responsibility;
- 6^{-th} level – All above and Business Continuity Management.

As demonstrated above, the creation of ISMS requires the efforts of specialists with knowledge and experience in numerous and different in nature and content subjects. At the same time, for the most part (if not everywhere) systems and methodologies for training of specialists and only include topics in the areas of physical and IT security, without considering the organizational aspects of security (including disciplines such as: Quality Assurance, Safety, Human Resources, Financial Security, Environmental Security, Social Corporate Responsibility, Business Continuity Management - exists only in the IT security, etc.). As for the ability to create practical application procedures for implementation of the elements of ISMS can from experience say that is achieved with hard work and profound knowledge. The lack of theory and practice in this field in the plans and programs of training institutions, is one of their weaknesses.

This is the purpose of this article, namely, the formulation of the range of issues that have additionally to be included in the plans and training programs for professionals who are involved in the design, construction, testing, operation and development of integrated security systems and protection of critical infrastructure. Of course it is a comprehensive process and will therefore allow me to narrow the range of subjects and to emphasize mainly on the requirements of professionals responsible for the design of these systems, taking into account the fundamental nature of this activity for the successful construction and operation of the latter. Of course, maybe there is no such specialization or position "Designer of Integrated Security Management System", but that does not mean that after a thorough discussion with the professional community, we can not create it.

STATE OF THE PROCESS OF TRAINING SPECIALISTS IN SECURITY

There are various methodologies and schools for the training of specialists who work or want to work in the field of security and protection of critical infrastructure. In an article like this can not be presented and analyzed all. But I will try to outline the trend in this area.

Above all, the efforts of training organizations are aimed at training students to the physical security of the infrastructure (this is conditional division, because there are no training programs for physical security, the trend is just focusing on this type of security). There are a number of disciplines, such as learning in the construction of buildings, access control, perimeter security, etc. Just as an example in this respect can be referred to the Facilities Standards for the Public Buildings Service (P100). This document establishes design standards and criteria for new buildings, major and minor alterations, and work in historic structures for the Public Buildings Service of the General Services Administration (US General Service Administration, 2003). In it, except on Structural Engineering, Mechanical Engineering, Electrical Engineering and Fire Protection Engineering are presented and issues of Security Design. Of course this is a standardization document requirements for the design and construction of buildings that need to be met by the designers and builders of buildings, but at the same time is the basis for the training of the past. There are many such documents, corporate, national or international, the combination of them, in order to train specialists in security depends on the leadership of the respective schools.

This direction - training in terms of physical security, is one of two main directions on which the stress in the preface of this article. Given the evolution of technology is difficult to say whether it dominates all other areas, but it can certainly be argued that it has the longest history in the development of theory and practice to ensure the security of the facilities. But this is not essential in this article, and the fact that such training is required, but not sufficient to ensure security and protection of critical infrastructure.

The other main direction in the training of security experts is training for the acquisition of knowledge and skills in the field of IT Security. Essentially, this activity involves mastering the requirements of ISO / IEC 27002 "Information technology - Security techniques - Code of practice for information security management" (and the related standardization and regulatory documents in this area). The last establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization (it comprises ISO / IEC 17799: 2005 and ISO / IEC 17799: 2005 / Cor.1: 2007). In the last decade huge leap in the development of information technology has accelerated development and methods for providing IT Security, which in fact, in many cases, exceeded the scope and dynamics of training in terms of physical security. In povarzhdenie of this finding is the structure of ISO / IEC 27002, which includes, among other things, and addressing issues such as: Asset Management, Human Resources Security, Physical and Environmental Security, Access Control, etc.

In general, the process of building an Electronic Security System passes through four distinct phases: conceptual design, design development, vendor selection and construction administration (Daniel M. O'Neill and Douglas Early, January 2012). On this basis have created a number of cocks for training, such as: CISSP Training Course, CEH Training Course for Certified Ethical Hacker Certification, ISO27001 Certified ISMS Lead Implementer Masterclass, CISA - Certified Information Systems Auditor Training Course, etc..

And this is natural because basically the development of mankind increasingly depends on the progress of information technologies.

But as well as physical security, training of specialists in IT Security does not cover all topics that are relevant to the development of integrated systems for security and protection of critical infrastructure and all objects that require the provision of security and protection. In confirmation of this are the following lines of this section of the article.

Global Security Services group, which brings together organizations that have developed and conducted a number of courses for certified security officers, but not only acknowledges that Security consultants and system designers are confronted with a wide array of certification options in both the physical and the Information Technological worlds (securityspecifiers.com, 2015).

In witness of the above, these organizations organize training courses for security specialists who acquire these certificates after successfully passing exams of the training:

- International Advancing Security Worldwide (ASIS):
    - Certified Protection Professional (CPP);
    - Physical Security Professional (PSP);
- BICSI – advancing the information and communication technology community:
    - Electronic Safety and Security (ESS);
    - Registered Communications Distribution Designer (RCDD);
- The Construction Specification Institute Construction:
    - Documents Technologist (CDT);
    - Certified Construction Contract Administration (CCCA);
    - Certified Construction Specifier (CCS);
    - Certified Construction Product Representative (CCPR);
- Electronics Technicians Association:
    - Electronic Security Networking Technician (ESNT);
- International Association of Professional Security Consultants:
    - Certified Security Consultant (CSC);
- Inspiring a Save and Secure Cyber World:
    - Certified Information Systems Security Professional (CISSP); and
- Security Industry Association (SIA):
    - Certified Security Project Manager (CSPM).

If we look closely at the name, but also in the content of the above courses, we see that each of them considered solely on individual aspects of the physical and / or IT Security. Only CSPM course assumes that students have transferred knowledge and experience in all areas of security and protection, not only in terms of physical and IT Security, but overall, ie, the integrated security system! But is that so?

If we look at the definition of the SIA for CSPM will see that the course contains: „The SIA Security Project Management Training Seminar gives security project managers the tools to execute projects efficiently and mitigate the risks for your clients and company“ (Security Industry Association, 2015). This course is only for Project efficiency and mitigation the risks, nothing more, i.e. nothing for the integrity of the activities that need to be taken into account when building management system of the organization and in the case when building integrated security system.

In support of the above, and the contents of the course, which includes (Security Industry Association, 2015):

- The self-study prerequisite courses cover the following topics:
    - Project Management Fundamentals;
    - Background for CCTV Systems and Applications;
    - Background for Access Control Systems and Applications;
    - Background for IP Systems and Applications;
    - Bidding Case Study;
    - Understanding Financial Statements.
- The CSPM training program curriculum consists of the following one-day classroom courses:
    - Security Project Management;
    - Estimating Security Projects;
    - Contracts, Codes and Risk Management;
    - Project Financial Management;
    - Managing the Project Team.

As we all see from what has been said here in this stage of the existing training courses for specialists and managers in the security of critical infrastructure (and not only) focuses on the acquisition of knowledge and experience in the areas of physical and IT Security. Training in the establishment and maintenance of integrated security systems, not be organized and conducted, ie, a large part of the organizational aspects of security, such as: Quality Assurance, Safety, Human Resources, Financial Security, Environmental Security, Social Corporate Responsibility, Business Continuity Management, etc. not included as subjects in the curricula.

NEED TO IMPROVE THE PROCESS OF TRAINING SPECIALISTS IN SECURITY

I think, to improve the training of professionals and managers in the security and protection of sites of critical infrastructure, in order to acquire knowledge and skills for construction and maintenance of integrated security systems, it is necessary to choose one of the following approaches:

- training for all security-related disciplines, ie, professionals to be trained by existing training programs and plans in terms of disciplines: Risk Assessment, Internal Security, External Security, Quality Assurance and Safety, Information Security, Human Resources, Financial Security, Environmental Security and Social Corporate Responsibility and Business Continuity Management;

- training that includes selected parts of the above disciplines enshrined in standardization and/or regulations or existing plans and programs, ie, using the method "tailoring”; or
- the creation of an entirely new, standardized at international level training program for construction and maintenance of integrated security systems.

Unlike the article; Alternative Method for Establishing of Security Levels, Journal of Applied Security Research (Stoichev K., 2015), where I presented the idea that the construction of the security levels of the integrated security system is preferable to using a single international standard document that be developed by the professional community here would like to propose an approach "tailoring". Of course keep in mind that the best from each perspective, and especially in terms of system approach is the creation of entirely new, internationally standardized training program for construction and maintenance of integrated security systems. Only in this way will create a reliable basis and criterion for assessing the ability of the organization to ensure the establishment of its desired levels of security and protection. This approach (standardization of international processes in the area, in case security) is the basis of the assessment and certification of the level of compliance with certain requirements in different areas of social and economic and social life of society. In this case it is the assessment and certification on the basis of uniform criteria for the level of success of the students in the mastery of knowledge and experience for building integrated security systems.

But this is a long process that will take a long time for its implementation, and the dynamics of the development of terrorist threats of any kind not wait. We are all witnesses of the creation in 2014 the Islamic state in the Middle East and the terrorist act of Al-Qaeda in Paris against the employees of the French satirical magazine "Charlie hebdo" in January 2015 in Paris. These are just two of the many cases in which terrorism has shown that it can accept all forms and to implement terrorist attacks worldwide.

As the first approach, training for all security-related disciplines, I would not recommend to be applied especially in terms of the need for an extended period of time to manage by one person or by all professionals of all security-related disciplines and because of the huge costs that have to be provided. And here is the place to mention that when we talk about education, I mean experts and individual manager, ie, what should be his training to be able to participate adequately in the development of integrated security systems. Certainly in priektniya team building of the system should be involved specialists in different disciplines listed above, but not every one of them or Project Manager to be trained in all disciplines combined. Appropriate and only in high risk sites of critical infrastructure (eg nuclear power plants) where security must be provided at the highest level with all available means and in all known ways. But even in these cases the need for continuous training of professionals or part of them in all subjects is unacceptable (funds in these cases are irrelevant, but training time is a crucial factor - the terrorists will not wait to be trained in all disciplines).

But back approach "tailoring". Its essence consists in from all disciplines take these requirements, which we believe relate to the construction of an integrated security system. It is preferable because of the following positive aspects:

- Exceptional flexibility and adaptability, which account the specificities of relevant organizations. In this event with success can that be applied and approach "Committed expenses - received Effects ", i.e. to found - best embodiment, wherein which planned results learning to be obtained with the best combination of financial, human and material resources;
- Brief time (compared with the first and the third approach), in which can that be trained professionals and managers;
- Relatively small, acceptable for most organizations, the financial resources needed for training.

But which of the above disciplines must be the linchpin to integrate knowledge from other disciplines related to the provision of the business?

I think this is Business Continuity Management (BCM) and it is wrong that this course is part of the ISO / IEC 27002 "Information technology - Security techniques - Code of practice for information security management" (this fact brings a certain ambiguity in the specialists, which is leading the construction of integrated security systems - BCM or IT Security). Rather, this standard should be part of the BCM. Why? Just because virtually no other subsystem except BCM system in which one way or another included mandatory requirements in relation to the other subsystems (in this case of the above disciplines, which set out the requirements for the subsystems) of the management system of the organization.

For example, the BCM system has absolutely all the elements of the structure of the system for quality management and using its methodology in the process of its own construction. Placing requirements subsystems for environmental management, health and safety, human resources, information technology and data protection, corporate social responsibility, risk management, are prerequisite for the development of policy, strategy and plans for BCM. And most of all, a serious section of this system borrow management requirements of the financial subsystem management system of the organization (as opposed to quality management, where these requirements are only touched upon). Requirements for this subsystem, refracted through the requirements to communication and information systems are extremely detailed and targeted, and what determines my comment that in the case of providing security and protection should be leading standards BCM, not IT standards.

Of course, evidence of the thesis that the BCM system is the integrating link in the Management System of the organization are numerous and easily verifiable, as I presented some of them in a number of other publications (Stoichev K., 2014, 10).

At the same time, BCM introduced Business Impact Analysis (BIA), which complements the Risk Assessment (RA), thereby providing the specialists who plan and design the construction of integrated security systems, a great tool to ensure the desired level of security . In support of this assertion is the fact that the BIA explores the events that lead to significant interruptions while RA examine all potential events that may affect the business of the organization, ie, both the analysis are two sides of the "the same coin" and complementing each other ensure the achievement of the planned security.

That is why professionals who are involved in the design of integrated security systems as well as relevant managers should master the art of conducting and possess the ability to correctly interpret the results of the two analysis - BIA and RA. And generally, they must necessarily be trained in building a Business Continuity Management System, which, as already noted, is fundamental in the management system of the organization and there is also leading the design, construction and maintenance of integrated security systems. Therefore they must be trained in any of the following courses or their peers (ECP-601, 2003):

Disaster Recovery Institute International (DRII.org):

- ABCP (Associate Business Continuity Planner);
- CBCP (Certified Business Continuity Professional);
- MBCP (Master Business Continuity Professional);

Business Continuity Institute (TheBCI.org):

- ABCI (Associate of the Business Continuity Institute);
- MBCI (Member of the Business Continuity Institute);
- FBCI (Fellow of the Business Continuity Institute);

National Institute for Business Continuity Management (NIBCM.org):

- ACM (Associate Continuity Manager);
- CCM (Certified Continuity Manager).

In which of these courses must be trained professionals is relevant decision of the management of the organization. But only in training them in itself is not enough. It must be supplemented with relevant topics in Risk Assessment (this discipline is taught in courses BCM), Internal

Security, External Security, Quality Assurance and Safety, Information Security, Human Resources, Financial Security, Environmental Security and Social Corporate Responsibility.

However, the inclusion of those subjects or of a part thereof in training of professionals is not sufficient. This approach includes only the organizational part (see the beginning of this article) in the construction of integrated security systems. What about the training of professionals capable of developing the technical part and writing procedures for the implementation of each of the activities related to security and defense? As already mentioned, not all of the team to build the system can know everything, for this purpose there are specialists in different disciplines and subsystems of the management system of the organization. But I think two people should have at least general knowledge of all subjects relating to the provision of security and protection of critical infrastructure. This is the Designer of Integrated Security Management System and Security Project Manager. Both should make sure you have knowledge and experience in the establishment of the organizational part of the system. As for the technical part, the Designer must master, above all, the specificity of information technology, while the Project Manager needs to know how they should be managed for security purposes (IT are at the heart of building security systems). Someone will say that for that purpose, system administrators or engineers in the IT area. This will answer that "narrow" IT professionals should always have corrective in the face of security specialists, the latter is necessary to master the basic principles in the IT area. This is a must if we don’t want IT specialists always to offer us for building security systems to buy the most expensive "toys" in their area (this is the mentality of most of his colleagues who really deep knowledge in IT area). Namely security specialists must have the ability to make accurate analysis of cost-benefit and build security levels of the organization, taking into account its specific needs in this area. And such a security expert in this case must be the Designer, which laid the foundations of the security system.

As for writing the procedures for implementation of security, it is necessary to be specific trained professionals with the Designer to participate in the construction of the system (the Designer is not able to do everything himself).

Only after the inclusion of the above subjects in the curricula and training programs for security specialists, taking into account the technical and procedural aspects of the construction of integrated security systems, we can talk about Certified Protection Professional, Certified Security Designer, Certified Security Project Manager and etc. That is, we need "integrated" training for professionals involved in the construction of integrated security systems of critical infrastructure.

CONCLUSION

Reflections presented in this article is not a criticism of existing methodologies and training schools of security specialists. This is an attempt to try to satisfy the needs of the dynamic and rapidly changing environment of terrorist threats. Technology (organizational and technical aspect) are in the process of continuous development and the means by which terrorists may affect the socio-political and socio-economic life of society every day increased. We should not be "catching up" in this race and to increase their chances for successful preventive action against terrorism must be at least "one step" to the knowledge, experience and capabilities of potential terrorists threaten our health or to take someone's life. This can and should be done primarily through the training of our staff, committed to providing security and protection of the organization. Only through "integrated" training we can be sure that the level of security that we want for ourselves and for the organization in which work can be achieved at the desired time and the planned price. Otherwise, or we will have options when built security systems can not resist terrorist threats (examples are numerous in this respect), or those cases in which we reinsure a very high price, which in turn does not guarantee 100% security.

Of course, the approach is not a panacea and if we want to move forward successfully in the field of training in this area it must be carefully and thoroughly discussed by the professional community, which define the scope and content of the curriculum for each post security . But that we need to apply such an integrated approach, I'm sure!

REFERENCES

Daniel M. O'Neill and Douglas Early, (January 2012), How to Design an Electronic Security System, http://www.facilitiesnet.com/security/article/How-to-Design-an-Electronic-Security-System-12954.

ECP-601, Effective Business Continuity Management, Institute for Business Continuity Training (2003), www.IBCT.com

Securityspecifiers.com; http://www.securityspecifiers.com/ResourcesCertsProf.asp.

Stoichev K. (2014, 10), The Role of Business Continuity Management in the Business Management System, Science Journal of Business and Management, 2014, 2(3), 97-102, DOI: 10.11648/j.sjbm.20140203.12

Stoichev K., (2014, 1), Integrated model for security and protection of critical infrastructure, Open Access Library Journal, Volume 1, e1124. http://dx.doi.org/10.4236/oalib.1101124.

Stoichev K., (2014, 2) Security Levels of Critical Infrastructure, Journal of Applied Security Research, 9:3, 328-337,DOI: 10.1080/19361610.2014.913233.

Stoichev K., (2015, 3), Alternative Method for Establishing of Security Levels, Journal of Applied Security Research, Volume 10, Issue 1, January 2015.

US General Service Administration, (2003), Facilities Standards (P100), http://www.gsa.gov/portal/category/21049.

Vitanov L. and Project team by NDA, Stoichev K. and Project team by IMSETHAC-BAS (2013), “Modeling of advanced system for security and water channelsprotection of the NPP”, Collection of materials with the results of the project: *"development of tools needed to coordinate inter-sectoral power and transport CIP activities at a situation of multilateral terrorist threat. increasing of the protection capacity of key CIP objects in BULGARIA– BULCIP",* ISBN 978-954-92552-6-3, 2013.

Yachev R. and Project team by NDA, Stoichev K. and Project team by IMSETHAC-BAS (2013), "Development of a security and protection model of the airport external perimeter", Collection of materials with the results of the project: *"development of tools needed to coordinate inter-sectoral power and transport CIP activities at a situation of multilateral terrorist threat. increasing of the protection capacity of key CIP objects in BULGARIA– BULCIP",* ISBN 978-954-92552-6-3, 2013.