GUIDO GLUSCHKE
PROF. DR. MESUT HAKKI CAŞIN
MARCO MACORI (EDS.)

CYBER SECURITY POLICIES AND CRITICAL INFRASTRUCTURE PROTECTION

CYBER SECURITY POLICIES AND CRITICAL INFRASTRUCTURE PROTECTION

Guido GLUSCHKE, Prof. Dr. Mesut Hakkı CAŞIN,

Marco MACORI (Eds.)

ISBN 978-3-00-058988-1 (print)

ISBN 978-3-00-060505-5 (pdf)

Institute for Security and Safety GmbH
David-Gilly-Str. 1
14469 Potsdam
Germany

Phone: +49 331 58148330
Email: info@uniss.org
Web: www.uniss.org

TABLE OF CONTENTS

CIP SECURITY AWARENESS AND TRAINING: STANDARDS AND PRACTICE

Rafał LESZCZYNA

ABSTRACT

These are critical infrastructure employees who have access to the critical cyber assets in the first place. This situation is well recognized by international and national standardization bodies which recommend security education, training and awareness as one of the key elements of critical infrastructure protection. In this chapter the standards are identified and their relevant areas are described. A practical implementation of the recommendations by means of a university course is presented.

Key Words: CIP, Training, Awareness, People Factor, Education

Introduction

Security experts agree that people are the critical factor in protection of the organization's cyber assets. The end-users access the assets on a regular basis and in most cases either they lack the security knowledge necessary to protect them or they know how to avoid protection mechanisms – in both cases the result is the same, namely the exposure of the cyber assets to threats.[246]

At the same time the majority of organizations concentrate their information security budget on technical solutions. This is because technical methods are well-defined (thus – comprehensible) and give an illusion that when applied all security issues will be solved. Acquire a "box" – an anti-virus, a firewall or an anti-malware – install it, and consider the problem solved.[247]

This approach tends however to be ineffective. Surveys show that despite the gradually increasing investments in technical controls the number of intrusions reported annually also continues to rise. Interestingly, there are reports claiming that the majority of breaches were caused by insiders. Technical solutions cannot make a network more

[246] Stephanie D. Hight, "The Importance of a Security, Education, Training and Awareness Program," 2005.
[247] Motorola, "The User Role in Information Security," 2010.

secure than activities of people who use it, because poor user practices overcome even the most carefully planned security system.[248]

Educating and raising security awareness among personnel is like expanding the information security department into the whole organization. Instead of few security experts trying to protect the network, security manager has at his/her support each employee of the organization taking care of the security interests of the company. This establishes some sort of a “human firewall” that will be very likely more efficient than a technical solution, and in contrast to it, able to recognize unknown, previously undetected threats.[249]

The importance of Security Education, Training and Awareness (SETA) is today widely recognized in the cybersecurity domain. The relevant security requirements and controls are described in majority if not all of security standards. The number of SETA initiatives continues to grow.[250]

In this chapter security requirements and controls in the standards most relevant to Critical Infrastructure Protection (CIP) are presented, followed by a description of a case study: teaching information security management (including CIP) at technical university in Poland.

Definitions

Security awareness is defined as set of activities that promote security, establish accountability, and provide personnel with updated information on threats, vulnerabilities, security solutions and so on.[251] It should result in that any individual who has access to the organization’s information assets is aware of potential consequences and his/her responsibilities.

Information security training aims at developing relevant security knowledge and skills within the workforce. It supports competency evolvement and aids personnel in understanding and learning how to perform their security functions. The most important difference between training and awareness is that the objective of training is to teach skills that allow a person to perform a specific role, while awareness aims at focusing an individual’s attention on a certain issue.[252]

Role-based training provides security courses that are adjusted to the particular needs of any group of people with significant responsibilities for information security in their organization.[253]

[248] Motorola, ibid.
[249] Motorola, ibid.
[250] Stephanie D. Hight, ibid.
[251] Pauline Bowen, Joan Hash, Mark Wilson, “NIST SP 800-100 Information Security Handbook: A Guide for Managers.” Gaithersburg, USA, 2006.
[252] Pauline Bowen, Joan Hash, Mark Wilson, Ibid.
[253] Pauline Bowen, Joan Hash, Mark Wilson, Ibid.

Security education aims at creating specialists and professionals capable of designing new security solutions and acting proactively. It integrates security skills and competencies from various functional areas and extends it with a multidisciplinary study of concepts, issues, and principles (technological and social). It is delivered as part of higher education.[254]

Critical Energy Infrastructure Standards: The Role of Education and Awareness Raising

Critical Infrastructures

Critical infrastructures consist of the physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments.[255]

In European Union a critical infrastructure is defined as an '*asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*'.[256]

The American definition of the term refers to '*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters'.*[257]

[254] Pauline Bowen, Joan Hash, Mark Wilson, Ibid.

[255] Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism (COM(2004) 702 final).

[256] Council Directive 2008/114/EC of 8 December 2008 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, L345/75.

[257] USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), section 1016(e).

Table 1. Critical infrastructure sectors depending on the classification

Critical infrastructure sectors	
European classification[258]	**American Classification[259]**
Energy installations and networks	Chemical
Communications and information technology	Commercial Facilities
Finance (banking, securities and investment)	Communications
Health care	Critical Manufacturing
Food	Dams
Water (dams, storage, treatment and networks)	Defense Industrial Base
Transport (airports, ports, intermodal facilities, railway and mass transit networks and traffic control systems)	Emergency Services
Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)	Energy
Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments)	Financial Services
	Food and Agriculture
	Government Facilities
	Healthcare and Public Health
	Information Technology
	Nuclear Reactors, Materials, and Waste
	Transportation Systems
	Water and Wastewater Systems

From various sectors recognized as critical (see e.g. two classifications in Table 1) the energy and transport are depicted as of the highest priority.[260]

[258] COM(2004) 702 final.

[259] Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience.

[260] Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/0786 final).

Critical Energy Infrastructures Cyber Security Standards

The number of standards and guidelines which to a greater or lesser extent refer to the cybersecurity of critical energy infrastructures is fairly high, which results in the situation that sometimes it is difficult to orientate oneself in this plethora of publications.

ENCS STUDY

Addressing this challenge, in 2013-2014 the European Network for Cyber Security (ENCS) conducted a study which aimed at the identification of standards which are the most relevant to the security of smart grids and smart grid Distribution Service Operators (DSOs).

The study, based on the previous investigations of various institutions (e.g. CEN, CENELEC, ETSI, ENISA, etc.) resulted in the identification of 11 publications enlisted in

Table **2**.

Table 2. CIP energy cybersecurity standards

Publication	Type	No. of occurrences in the studies
IEC 62351	Standard	5
NERC CIP	Regulation	4
IEC 62443 (ISA 99)	Standards and guidelines	4
IEEE 1686-2007	Standard	4
ISO/IEC 27001	Standard	3
NISTIR 7628	Guideline (Technical Report)	3
NIST SP 800-53	Guideline (Special Publication)	3
IEC 62357	Technical Report	2
ISO/IEC 27002	Standard	2
NIST SP 800-82	Guideline (Special Publication)	2

DHS Catalog	Guideline (Technical Report)	2

ENISA Studies

Critical infrastructures, such as electricity generation plants, transportation systems, oil refineries, chemical factories and manufacturing facilities are large, distributed complexes. The majority of them uses Industrial Control Systems (ICS) for monitoring and control. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems.

In 2011, the European Network and Information Security Agency (ENISA) conducted a study in the domain of ICS and SCADA. Its objective was to obtain the view on the ICS protection primarily in Europe but also in the international context. The study based on the previous work done in the ESCoRTS project, and specifically on “D2.1 - Survey of Existing Methods, Procedures and Guidelines” recognized around international or significant national standards and guidelines dedicated to ICS. The study was followed in 2012 in reference to Smart Grids and resulted in the identification of further ICS standards and guidelines. The results of both studies are presented in Table 3.

Table 3. Standards and guidelines dedicated to industrial control systems identified in the ENISA studies

Standards and guidelines dedicated to industrial control systems	
IEC 62351. Data and communications security	IEEE 1686-2007. Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
IEC 62210. Power system control and associated communications - Data and communication security	IEEE 1402. Guide for Electric Power Substation Physical and Electronic Security
IEC 62443. Security for Industrial Process Measurement and Control: Network and System Security	IEEE 1711. Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links
Security Profile for Advanced Metering Infrastructure	ISO 27000
ISO/IEC 15408, Evaluation criteria for IT security (also known as “Common Criteria”)	ISA 99. Manufacturing and Control System Security

Cyber Security Assessments of Industrial Control Systems. A good practice guide	Configuring & managing remote access for industrial control systems. A good practice guide
Good practice guide - Process Control and SCADA Security	Firewall deployment for SCADA and process control networks. A good practice guide
Process Control Domain (PCD) – Security Requirements for Vendors	NAMUR NA 115. IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries
VDI/VDE 2182 Series	OLF Guideline No. 104. Information security baseline requirements for process control, safety and support ICT systems
OLF Guideline No. 110. Implementation of information security in Process Control, Safety and Support ICT Systems during the engineering, procurement and commissioning phases	CheckIT
CRIOP	Guide to Increased Security in Industrial Control Systems
NIST SP 800-82. Guide to Industrial Control Systems (ICS) Security	NIST SP 800-53. Recommended Security Controls for Federal Information Systems
NISTIR 7176. System Protection Profile - Industrial Control Systems	Field Device Protection Profile for SCADA Systems in Medium Robustness Environments
AGA Report No. 12. Cryptographic Protection of SCADA Communications	API 1164, Pipeline SCADA Security
API Security Guidelines for the Petroleum Industry	21 Steps to Improve Cyber Security for SCADA Systems
Catalogue of Control Systems Security: Recommendations for Standards Developers	Securing your SCADA and Industrial Control Systems

ICS Standards

The standards address various aspects of security of industrial controls systems: data and communication security, security requirements and controls, risk management, security programs and other issues.

For instance, IEC 62351 and IEEE 1711 focus on data and communication security. IEC 62351 introduces security measures to protocols used in the energy sector, such as IEC 60870-5 (DNP3, IEC101, IEC104) or IEC 60870 (TASSE.2/ICCP). IEEE 1711 defines a cryptographic protocol to provide integrity and optional confidentiality for cyber security of serial links.[261]

NERC CIP, DHS Catalogue of Control Systems Security, NIST SP 800-53, ISO/IEC 27001 or ISA/IEC 62443[262] are industry-recognized standards which describe security requirements and controls which are essential for building a security framework in a system as they explicitly define security measures which must be present in the system in order to assure its protection.

Knowing the controls and requirements, operators can request specific security functions from vendors in the products they offer. They can also consider appropriate criteria when making purchasing decisions. For instance, IEEE 1686-2007 defines the functions and features to be provided in substation IEDs to accommodate Critical Infrastructure Protection (CIP) programs. Another example are “WIB Security Requirements for Vendors”, which provide requirements and recommendations for IT security to be fulfilled by vendors of process control and automation systems.[263]

Another group of publications is devoted to risk management related concepts and methodologies, and includes, for example, ISA-62443-3-2, or NISTIR 7628, which is based on NIST SP 800-39, NIST SP 800-30, FIPS 200, FIPS 199, NERC Vulnerability and Risk Assessment and other documents.

For an enterprise, a very important aspect of cyber security is to establish an Information Security Management System (ISMS). There are very few documents which advise operators on how to incorporate industrial control systems into their ISMS. One of them is IEC 62443-2-1, which adapts the relevant content of ANSI/ISA 99, defines the elements necessary to establish a cyber security management system (CSMS) for ICS and provides guidance on how to develop those elements. The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

[261] ENISA, “Protecting Industrial Control Systems - Recommendations for Europe and Member States”, ENISA, 2011.
[262] ENISA, Ibid.
[263] ENISA, Ibid.

Other documents that help operators develop such an ISMS system are API 1164 or a combination of the famous ISO/IEC 27000 framework with NIST SP 800-82. API 1164 provides pipeline SCADA operators with a description of industry practices in SCADA security, and a framework needed to develop sound security practices within the operator's individual companies.

ISO/IEC 27000 framework is composed of information security standards which provide recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS). The series is broad in scope and non-ICS-specific, aiming at organizations of all structures and sizes. For this reason it is necessary to use it in conjunction with other, more specific publication(s), for example NIST SP 800-82.

NIST SP 800-82 provides guidance on securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions. The document gives an overview of ICS and typical system topologies, identifies common threats and vulnerabilities and provides recommended security countermeasures to mitigate the associated risks. It also addresses specific security controls for ICS, provides enhancements to classic ones and a supplemental guidance for the controls which can be applied in a practically straightforward manner. NIST 800-82 is well recognized among the ICS users, providers and supporters (public bodies, standardization bodies, academia and R&D).[264]

Preliminary Cyber Security Framework

In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity. The framework aims at supporting critical infrastructure owners and operators in reducing cybersecurity risks in industries such as power generation, transportation and telecommunications. It relies on a variety of existing standards, guidelines, and practices and indicates them adequately to each area of critical infrastructure protection in the Framework Core. These references include publications such as: ISO/IEC 27001, NIST SP 800-53, ISA 62443, COBIT and CCS.

Cyber Security Education, Training and Awareness Raising in the Standards

Practically all standards which are not strictly technical but address higher level cybersecurity issues, such as security management or administration, underline the importance of actions related to education or training or awareness raising of users.

In this chapter we present the requirements or controls in the most relevant standards (see

Table **2**).

[264] ENISA, Ibid.

NERC CIP

NERC CIP-004-3 requires that all personnel (including contractors and service vendors) authorized to access critical cyber assets have an appropriate level of training and security awareness.

For this purpose a security awareness program must be implemented which includes security awareness reinforcement on at least quarterly basis using mechanisms such as:

- Direct communications (e.g., e-mails, memos, computer based training, etc.)
- Indirect communications (e.g., posters, intranet, brochures, etc.)
- Management support and reinforcement (e.g., presentations, meetings, etc.)

The awareness program should go hand in hand with a cyber security training program, reviewed and updated at minimum on annual basis. This program will ensure that all relevant personnel is trained before they are granted access to critical cyber assets and covers at minimum:

- The proper use of critical cyber assets
- Physical and electronic access controls to the assets
- The proper handling of asset information
- Action plans and procedures to recover from a cyber security incident

ISO/IEC 27001 and 27002

In ISO/IEC 27001, the A.8.2.2 security control (“Information security awareness, education and training”) imposes that all employees of an organization, contractors and third party users receive awareness training and regular updates in organizational policies and procedures relevantly to their job function.

ISO/IEC 27002 provides additional guidance on the implementation of the control. Awareness training should start with a formal introduction of the organization’s security policies and expectations. This must be done yet before access to critical information assets or services is granted. Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process.

The aim of the awareness raising activities is to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role. They must include information on known threats, contact person and the proper channels for reporting information security incidents.

ISA 99

In ISA-62443-2-1-WD the security control 8.2.2 ("Security awareness, education, and training") is specified which identically as in the 8.2.2 control from ISO/IEC 27001[265] requires that all relevant users receive awareness training and regular updates in organizational policies and procedures relevantly to their job function. "**This should include the information necessary to identify, review, address and where appropriate, remediate vulnerabilities and threats to Industrial Automation and Control Systems (IACS).**"

The standard provides implementation guidance and control enhancements **including the IACS-specific guidance**. The latest, among the others, imposes that IACS operators and maintenance staff should participate in the training.

Awareness training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of IACS facilities and information on the disciplinary process. A formal introduction of the organization's security policies and expectations must be given before granting the users the access to information or the IACS.

The security awareness, education, and training activities must be tailored to the skills and the role of a user and should include information on known threats and vulnerabilities, a contact person for further security advice and reporting channels for security incidents. All personnel must be instructed about social engineering techniques.

According to IEC/TR 62443-3-1, as part of a personnel security program, all employees, contractors, or temporary workers should be completely trained in their basic job responsibilities, the terms and conditions of their employment, disciplinary actions and appeal process, security requirements, and safety requirements. Each employee should be reviewed periodically and/or retraining must be settled down to ensure that employees remain aware of their job functions.

NIST IR 7828

The NIST IR publication recognizes security awareness as a critical part of information system incident prevention and dedicates to it the SG.AT (Awareness and Training) family of controls.

It requires from organizations:

- Designing effective training programs based on individuals' roles and responsibilities
- Developing, establishing and maintaining awareness and training security policy
- Performing basic security awareness briefings to all Smart Grid information system users

[265] ISA 99 is partially based on ISO/IEC 27001.

- Providing security-related training first before authorizing access to the information system or performing assigned duties and after that – periodically or induced by a substantial change
- Maintaining a record of awareness and training for each user
- Establishing and maintaining contact with security groups and associations to share security-related information including threats, vulnerabilities, and incidents and to be informed about the newest recommended security practices, techniques, and technologies

NIST SP 800-53

NIST Special Publication 800-53 in the family AT “Awareness and Training” defines four controls which impose:

1. The development, documentation and dissemination of security awareness and training policy and procedures
2. Training of information system users (including managers, senior executives, and contractors) as part of initial training for new users and periodically thereafter
3. Provision of role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties and periodically thereafter
4. Documentation and monitoring of individual information system security training activities and retention of individual training records

For each control, supplemental guidance is provided as well as control enhancements when needed.

Besides the AT family, there are several controls defined in other families which refer to security education, awareness and training.

PM-13 “Information security workforce” requires the establishment of an information security workforce development and improvement program.

PM-14 “Testing, training, and monitoring” ensures that an organization provides and coordinates security testing, training, and monitoring activities. These activities must be informed by current threat and vulnerability assessments.

CP-3 “Contingency training” and IR-2 “Incident response training” impose the provision of contingency and incident response trainings.

SA-16 “Developer-provided training” ensures that (external or internal) developer of the information system, system component, or information system service to provide training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

NIST SP 800-82

According to NIST SP 800-82: "Many of the interconnections between corporate networks and ICS require the integration of systems with different communications standards. (…) Because of the complexity of integrating disparate systems, control engineers often fail to address the added burden of accounting for security risks. Many control engineers have little if any training in security and often IT security personnel are not involved in ICS security design. As a result, access controls designed to protect control systems from unauthorized access through corporate networks are usually minimal."

The quasi standard recognizes security awareness as a critical part of ICS incident prevention, in particular in reference to social engineering. Thus it recommends providing training and raising security awareness as part of security program development. The training and awareness activities will facilitate the implementation of an ICS security program as they prepare the employees for changes resulting from it. They also demonstrate management's commitment to a cyber security program. Feedback from personnel participating in the training can be a valuable source of information for improving the security program.

NIST SP 800-82 security controls for awareness and training direct a reader to the Awareness and Training family from NIST SP 800-53 in the first place. Additionally the following publications are indicated:

- NIST SP 800-12 – for guidance on security policies and procedures
- NIST SP 800-16 – for guidance on security training requirements
- NIST SP 800-50 – for guidance on security awareness training
- NIST SP 800-100 – for guidance on information security governance and planning

NIST SP 800-82 provides an ICS specific recommendations and guidance on security awareness and training, which among the others, imposes the inclusion of control system-specific information for specific ICS applications into the awareness and training program as well as the need of training of all personnel having significant ICS roles and responsibilities. The program must cover the physical process being controlled as well as the ICS.

Case Study: Teaching Information Security Management at Technical University

Recognizing the importance of security awareness in enterprises and organizations especially those which belong to critical infrastructures, the information security management course was introduced in 2010 into the curriculum of students of the Faculty of Management and Economics at Gdańsk University of Technology. The aim of the course is to introduce a student with the fundamentals and key concepts of information security management, with a particular attention to the security management lifecycle. The formula of the course is conceptualized in the way that during laboratory exercises students, working in groups, pass the subsequent phases of the lifecycle, starting from choosing an enterprise which will undergo the phases and concluding with designing adequate security controls (whether technical, administrative or physical). The laboratory work is accompanied with a lecture which aims at introducing the relevant knowledge beforehand. There are fifteen hours of lecture and thirty hours of lab in a semester.

Lecture

The contents of the lecture are as follows:

- Introduction: the context of information security, knowledge based economy, the growth of number and complexity of attacks, problems and challenges, critical infrastructures, NIST and ISO, legal requirements, definitions of basic security terms
- Cost of the information security management in an enterprise: rationale, key premises of management decision, scarcity of security cost assessment methods, brief review of existing methods
- Information Security Management System (ISMS): explanation, lifecycle
- Standard ISO/IEC 27001: key characteristics, ISMS, PDCA model, detailed explanation of the four phases of the ISMS lifecycle, Annex A – control objectives and security controls, example-based explanation of a security control
- NIST Special Publication 800-53: NIST document types (standards, special publications, others), NIST partners and consultants, NIST SP 800-53 objectives, security controls, example-based explanation of a security control, baseline controls, risk management framework, FIPS 199 and 200
- Information security management process in accordance with ISO/IEC 27001 and NIST SP 800-53
- Information security policy
- Security threats: descriptions and taxonomies
- Risk management: introduction, basic concepts (risk, threat, vulnerability etc.), frameworks and standards, lifecycle, risk analysis methods, detailed explanation of the simplified qualitative risk assessment method
- Technical security controls: firewalls, cryptography, identification and authentication, access control, intrusion detection systems
- Physical security, personnel security, information security awareness and training

During the lecture the importance of securing critical infrastructures is explained and several vivid examples of scenarios of attacking the infrastructures are presented including Stuxnet, Flame or a fictional attack on the U.S. Nation’s Critical Infrastructure.

Lab

The lab work constitutes the core of the security management course. The lessons go in parallel to the lecture, but their contents are postponed to the lecture, so the students are introduced to each subject. This is possible, because in the first stage, students need to form groups and each of the groups must choose an existent enterprise or propose a fictitious one, for which they will perform all further analyses. Then the enterprise needs to be analyzed from the security point of view, so among the others to facilitate assessments of threat impact. Thus the business model and functioning of the enterprise must be analyzed in the first place, as depending on it, some information assets are more and some less important. Students describe the mission, goal, organizational structure and the main activities of the organization. Then they analyze the information system of the organization, describe it and prepare diagrams. All results are compiled into a report. This introductory part takes three weeks (2 hours a week). In the meantime, the students listen to the lecture about concepts necessary for the performance of further studies (cost assessment in that case).

During the next two weeks, students assess the cost of information security management in the enterprise. To do so, they determine values of a set of parameters characterizing the enterprise, such as the number of users, number of security professionals or hire rate. Based on the data, cost estimations are obtained. Students analyze the results and present the conclusions and the related data in a report.

Risk assessment constitutes the subsequent part of the lab exercises. Students identify all information assets in their organization, describe them and assess the impact of violating confidentiality, integrity and availability of these assets. Each student group analyses available security threat lists and taxonomies and prepare the list of threats adequate to their company. Then for six selected, according to a justified criterion, information assets, the students evaluate threat probabilities and assess risks. As for each part of the lab work, students consolidate the results into a report.

When students are aware of the security context of their organization, know the possible threats, their impact on the company business, and are able to systematize information assets based on the associated risks – they can prepare information security policy. The resulting policy document should be the outcome of the analysis of other available publications as well as effects of previous work.

The lab concludes with selecting security controls in accordance with the standard chosen between ISO/IEC 27001 and NIST SP 800-53. Students justify their choice of the standard and select the security controls for the six information assets selected during the risk assessment. They describe the controls and if applicable – present the control areas not addressed by the controls. Each group prepares the new diagram of the information system which incorporates technical security solutions. Finally the students describe their conclusions and observations.

To complete the course, students must participate in all five parts of the laboratory with adequate results and well written report. Besides, they need to pass the knowledge assessment which is based on open questions as well as multiple choice test. The questions include those which refer to critical infrastructures. For instance in the most recent edition of the course students had to explain the notion of critical infrastructure and indicate which attack discovered in 2010 targeted among the others Iranian nuclear facilities.

Conclusion

Recognizing the crucial role of users in Critical Infrastructure Protection, the cybersecurity standards used in the energy sector, such as NERC CIP, ISO/IEC 27001, ISA 99 or NIST SP 800-82, recommend designing and establishing Security, Education, Training and Awareness Programs (SETA), which define SETA policies, roles and responsibilities. The latest include direct and indirect communications or management reinforcement to bring the employees' attention to security issues (awareness raising), teaching specific security-related skills (training) or more long-term and multidisciplinary studies usually performed at universities (education).

The experiences from delivering an information security management course at Faculty of Management and Economics of Gdańsk University of Technology show the key role of practice in the education of information security. Assessments demonstrate that students more willingly refer to the knowledge and experiences obtained during lab exercises than the theoretical knowledge received from the lecture. With a course designed as a combination of lab work and a lecture, with the focus on the former, it is possible to achieve positive results of the assessments, indicating that students have sufficient level of information security awareness.

The information security management course was introduced to the curricula of students of management and economics because many of graduates will later take managerial and administrative positions in enterprises and organizations, and on their decisions will depend the cybersecurity condition in their companies. For this reason such a fundamental cybersecurity course should be provided in all academic institutions of a similar profile. The introduction of the course should be also discussed to the technical faculties linked to the infrastructures identified as critical, for example electrical and control engineering faculties or chemistry faculties.

REFERENCES

BOWEN, P., HASH, J., WILSON, M., “NIST SP 800-100 Information Security Handbook: A Guide for Managers”, Gaithersburg, USA, 2006.

Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism (COM (2004) 702 final.

ENISA, “Protecting Industrial Control Systems - Recommendations for Europe and Member States”, 2011.

Motorola, “The User Role in Information Security”, 2010.

Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience.

USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), section 1016(e).

HIGHT, S. D., “The Importance of a Security, Education, Training and Awareness Program,” 2005.