Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies

Aleksandar Klaić
Office of the National Security Council
E-mail: aleksandar.klaic@public.carnet.hr

Abstract - The overview of the field of information security (IS) policy and IS management methodologies is given in the paper. Key terms of the field are defined and contemporary trends of development are described. The need for the establishment of the IS governance level is analyzed, as well as the link between governance level and the security programs that are the basis for the implementation of information security management system (ISMS). The systemic security management model is described, where security is considered as a dynamically interconnected, multidimensional activity. Specifics of the contemporary IS policy and ISMS methodologies are determined in the context of the traditional IS policy approach that is typical for Government sectors, but also in the context of security programme frameworks established by the contemporary IS standards. The role of security metrics in the field of IS management is described, as well as the importance of metrics at the corporate and the operational management level.

I. INTRODUCTION

Information security (IS) policy is primarily determined by the environment in which various information is being used and communicated. Due to the rapid development of information and communication technology, as well as to widespread Internet connectivity, the complexity of the security environment has been hugely increased over the last twenty years. There is a need for change in approach in regards to the three key elements: people, processes and technology. This change was triggered by the new environment of general globalisation, by the increased dependence of the business processes on technology, and also by the transformation of a market oriented society based on private property, into an information society based on knowledge and information.

II. DEVELOPMENT OF THE FIELD

IS policy development, as it is recognizable today, began with the transition from the 1960s to 1970s. At that time IS policy was present almost exclusively within the segment of classified Government information, it was prescribed by the internal rules of security bodies, and it was closed to the public. Mutually confronted, public and secret information spaces, became transparent information domains over the next few decades because of the number of democratic and globalisation processes. The domains that are dominant today regarding IS requirements are: classified information, unclassified information, personal information, and intellectual property. Together with the democratic principle of public administration transparency – freedom of information, as well as the concept of e-Government, they characterise contemporary information space from the IS point of view [1].

IS policies as well as the security programmes for the implementation of the policy, basically differ in their object of protection. In the traditional approach to IS policy in the Government sector, the protected object is classified information. The established methodologies of protection apply to personnel, processes, and technology, within a framework in which such classified information is exchanged [2]. In the contemporary approach to IS management in the business sector, protection objects are information assets in a wider sense [3], or the business values and attributes [4], in which risk management methodologies are applied.

III. DEFINITIONS OF THE FIELD

The development of the field shows the great extent and the complexity of the content of the contemporary IS policy. In order to approach to all these different fields in a comprehensive way, and to analyse the requirements that are used to define specific contents of the policy, it is necessary to establish the taxonomy of the key terms.

A. Information Security

Information can be generally defined as the data with meaning and purpose. The data can be in the shape of document, or any other record, cognition, or practise, oral communication etc. The knowledge represents organized information that are stored, controllably distributed, and legally protected in a proper way, which is very similar to the concept of intellectual property [7].

Information security is the state of information confidentiality, integrity, and availability that is established by the implementation of prescribed measures and standards, and by the organization support for the activities of planning, implementation, checking, and improving of the measures and standards [6].

B. Information Space / Cyber Space

Information Space represents public communication and information space, within the meaning of connection of all computer networks, databases, and generally all types of sources of information. In that way it is the virtual network environment which is global and populated with knowledge in electronic shape [8].

Cyber Space, Cyber Security, Cyber Terrorism, Cyber Threats, all these terms are derivatives of the prefix “cyber”, which is originally used to form the term “cybernetics”. Cybernetics is the scientific study that deals

with automatic control systems and generally with control processes in biological, technical, economic, and other systems. The term Cyber Space has basically the same meaning as the term Information Space. The difference is in the usage. The term Cyber Space is more often used within the framework of computer incident response capabilities and computer crimes, whereas the term Information Space is more often used in the field of planning and implementation of contemporary electronic services, such as e-Government [10].

C. Information Society

Contemporary information society or knowledge society treats the intellectual property (information) in a similar way as market economy treats private property. This means that within a contemporary society, which is inseparable from the previously defined information space, it is not possible to isolate information. Information is freely communicated and exchanged.

D. Information Security Policy

NATO and EU use the term Security Policy within their security directives instead of the term Information Security Policy, and the same term in this narrow meaning can be found throughout the literature in information security field. It is important to stress that the term security policy has its wider meaning closely connected with the term national security. Contemporary security policies in their wider meaning are defined as the activities for assurance preparations from the sources of future threats in the nature, within society, and among the societies. In their narrow meaning, contemporary security policies represent the sum of all measures, activities and practises, designated to establish and operate the national security system [9].

In that sense IS policy represents all the documents that are used to establish IS measures and standards. These measures and standards have to be applied in the information space, in order to protect information confidentiality, integrity, and availability, and also availability and integrity of information systems that process, store or communicate that information.

The IS policy document in the narrow sense represents statement or declaration of the most important management persons (CEO, Executive Board, Minister …), about beliefs, goals, and reasons, and also general ways to accomplish desirable achievements in the field of information security. Such policy document is written in the form of short and concise document on general level, with no specifics and detailed descriptions. In wider sense, IS policy documents represent hierarchically structured set of regulation. This set of documents is comprised of described umbrella document, and several other layers: standards (binding requirements), procedures (binding actions), and guidelines (recommended ways of realization of standards and procedures) [11].

E. Information Criteria

It is not possible to separate the concepts of information security and security of information space. It stems from the previously introduced definitions. Therefore, the information society that started to develop in the 1990s, relentlessly led to using, not only security information criteria, but also the criteria of fiduciary and quality. Security criteria: confidentiality, integrity, and availability, were enough to describe isolated, classified information systems. But in the contemporary information space we also have to use criteria as: compliance, reliability, effectiveness and efficiency [1] [12].

F. Security Programme

Security programme is established in order to implement the IS policy. It includes planning, implementation, checking, and improving, but also the permanent management of key elements (people, processes, and technology), that can influence the security aspects within the framework of whole organization [4]. There are different sources of security standards that can be used in the security programmes development [3] [7].

G. Information Security Management System

Information Security Management System (ISMS) is a part of the overall management system, based on the risk management, and established with a view to implement, monitor, review, maintain, and improve information security [3]. ISO/IEC in the requirements of its standards determine the use of the life cycle process - Plan, Do, Check, Act (PDCA) - when establishing and using ISMS. Process represents the set of interdependent actions and activities that are done with a view to achieve predetermined set of products, results, or services.

H. Risk Management

Risk management represents coordinated activities that direct and manage organization in the sense of its risks. This term usually encompasses risk assessment (analyses and evaluation), risk treatment (choosing of best way), and risk acceptance (statement of the executive board).

Risk represents the combination of the event probability and its consequences (impact). Threat is potential cause of the unwanted incident that may harm to system or organisation. Vulnerability is the weakness of some asset or set of assets that may be used by threat [3].

I. Security Controls, Measures and Standards

Security controls are processes that assure to an organization the fulfilment of the set goals of confidentiality, integrity, and availability [13]. Security controls are often used as the synonym for the terms protections and countermeasures. Security controls represent the way of controlling risks, which includes policies, procedures, guidelines, or practises, that can be of administrative, technical, organizational, or legislative character.

IS measures are general rules of information protection that are realised on physical, technical, or organisational level. IS standards are organisational and technical procedures, and solutions intended for systematic and balanced implementation of prescribed information security measures [6].

J. Information Security Oversight

Taxonomy of IS oversight methodologies typically encompasses audit, assessment, inspection, and penetration testing. Audit is consisted of evaluation of ISMS, and it is performed according to a prescribed standard and documented process. Within the IS policy of the Government sector audit is usually called oversight. Assessment is the activity used as the qualified revision and it is typically performed in one segment of IS policy (e.g. vulnerability assessment). Inspection is a one-time checking of the organisation security posture at a specific time, and it is usually applied as a part of the audit process. Penetration testing is an evaluation methodology that tries to avoid security controls and obtain access to a specific information system, with a view to determine attack vectors (vulnerability-threat) with which it would be possible to compromise the security of the system.

Internal and external audit are distinguished, depending on the way how they are performed, by the organisation employees or by the external (independent) associates. These types of audits or oversights are mutually combined according to defined time schedule. A few ways of penetration testing are distinguished according to the similar principle, depending on what is comprised in testing, who performs the testing, and who is introduced with the performance of the testing.

Accreditation concept is generally defined as approval to operate within a business segment of an organisation. This means that the organisation takes the responsibility for the operation, in accordance to the specified standard, and the responsibility for risks in that business segment [2]. Certification concept is defined as an overall assessment of technical, organisational, and administrative controls, in order to verify if the controls are applied in accordance with accepted standard [3]. Accreditation and certification processes are based on described oversight methodologies.

K. Critical Information Infrastructure

Over the 1990's, in parallel with the development of contemporary information society, it was discovered that some key sectors of the society (Energy, Telecommunication, Financial, Water, Public health, Government facilities, etc.) contain the so-called Critical Infrastructure (CI). These key sectors are either vitally important for national security or crucial for economic and societal welfare of the nation. CI lies on the whole spectrum of mutually interconnected national and international information systems that are used in order to have successful and effective operation and control of such CI. Mutually interconnected national and international information systems are called critical information infrastructure (CII).

In that sense, CI is infrastructure which incapacitation or destruction would have had the weakening impact on national security, economic and societal welfare. CII is critical information infrastructure that underpins multiple elements of CI. Because information systems are in great extent mutually interconnected, or connected to public systems, CII is being more and more exposed, not only to failures and damages, but also to different types of malicious attacks, either accidentally (e.g. computer viruses), or intentionally (e.g. cyber terrorism). The necessity of recognizing CI stems from the basic CI problem, the fact that an attack to a CI, by itself, multiplies the force of attack. In that way a relatively small attack to an infrastructure object can have the huge impact and cause damage on a number of mutually connected infrastructure objects [10] [15] [17].

IV. METHODOLOGIES

Methodology is generally system of practises, techniques, procedures, and rules that are used in the field of specific discipline. Methodology is also the set of guidelines and principles that can be shaped and applied in specific situation, as well as specific approach, templates, and forms that are used throughout the management lifecycle of specific process.

In the paper traditional methodologies of IS management are briefly described. Comparison of traditional and contemporary methodologies is made, as well as an overview of some new development trends using hybrid approach. This hybrid approach combines the best characteristics of both the traditional and contemporary approaches. Contemporary security metrics approach is also considered in the paper, as well as some more important security metrics methodologies that facilitate better IS management.

A. Traditional Approach to Information Security Management

Traditional approach to *IS* management is based on stipulating the minimal security measures and standards that are determined according to the classification level of classified information. Protection measures are applied to classified information in any shape, to objects (technology and processes), and to subjects (people), that use or access to classified information [2]. This approach implies that classified information is exclusive protected object, and the methodology is applied to people, organisation (process), and technology, but only if they are in contact with classified information.

The basic concepts of this approach originated from 1960s, when clearer and clearer security policy requirements motivated the development of security models for performing the goals of security policy, primarily within the information systems. In this way the Bell-La Padula model, and the lattice model, were developed as models that elaborate access control to information stored on an information system, focusing on the criterion of information confidentiality. In difference from these models, the Biba model focused on the integrity criterion, and there are the number of other formal security models [16]. Security models adjust the architecture of information system to the goals of security policy in a formal, mathematical way.

As information system is consisted of environment that, besides technical system, encompasses the organisation responsible for that information system, stored information and users, the necessary step forward were security modes of operation. Security modes of operation of information systems are: dedicated, system high, compartmented, and multilevel. They connect the level of classified information stored within the information system, the level of person's security certificates, the "need-to-know" approach, and the

formal approval to access classified information within the information system [2]. These elements, from a security point of view, represent the basic elements that are needed to decide on assignment of the access to the system.

Requirements that are set up by the traditional approach to information security basically have static character. They are prescribed in advance and according to the classification level of classified information. IS policy is shaped following the experience and best practises, leaving no space for the specifics of the business environment. The mechanisms of the implementation are prescribed in detail, in order to have unified solutions in the very heterogeneous organisation of a Government sector (Fig.1.).

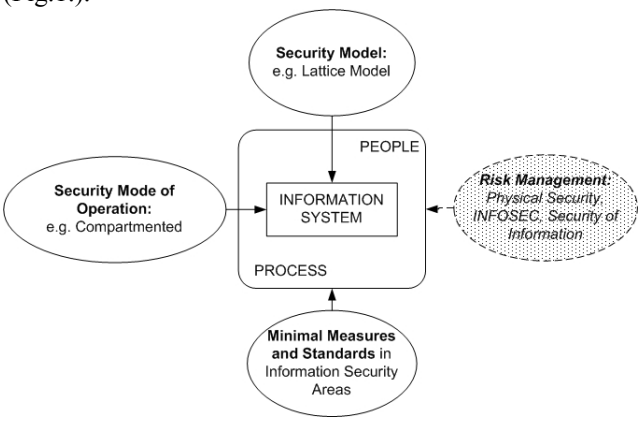

Fig.1. Traditional approach to information security management

B. Contemporary Approach to Information Security Management

Contemporary approach to IS management is based on risk management, while in the traditional approach risk management is only additional methodology that is being more applied recently [13] (Fig.1.). Risk management methodologies are based on identified information assets that are within the scope of ISMS, on assessed threats to these assets, on assessed vulnerabilities that can be used by threats, and on the assessment of the possible impact of the loss of confidentiality, integrity, and availability of the assets [3] [7]. Security controls protect identified assets, as valuables that are identified within the scope of ISMS. Basic concepts of risk management in the field of information security started to be applied wider by the end of 1990s.

The requirements that are set up by the contemporary IS management approach have dynamic character, which means they are adapted according to periodically based risk assessment. Additionally, the results of the risk assessment are related to the particular security environment, and are optimally adapted to the real combination of threats and vulnerabilities of particular assets. Security controls for elimination or mitigation of risks, usually are not prescribed in detail in order to enable the adjustment of implementation to different security environments of legal persons in different countries that can use the international standards. The process of risk assessment is based on subjective evaluation and therefore the complete calculation of key risk values is subjective. Incomplete data on the frequency of security threats occurrence, as well as the calculation of very rare threats, further contributes to subjectivity and inaccuracy of the risk calculations.

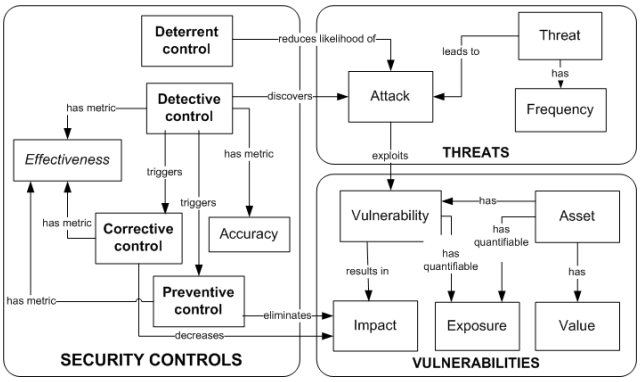

Fig.2. Logical model of security controls

C. Trends of the Development in Information Security Management

The development of the field of IS management is directed today towards multidimensional conception of IS policy (interdependence of the policy domains). Second important direction is to include some factors that have not been thought of as security relevant in traditional approach (e.g. organisational culture). The third direction of development is being concerned with the problem of subjectivity in risk management, as the biggest weakness of the contemporary approach to IS management (e.g. the development of security metrics).

a. Information Security Governance

Governance is the set of responsibilities and practises exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly (Fig.3).

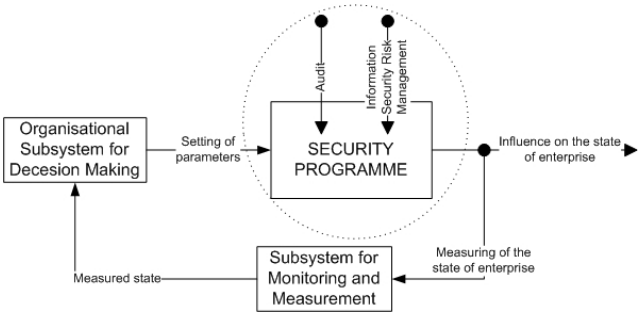

Fig.3. Information Security Governance

IS governance in this way direct IS programme toward the goals defined at corporate level, but it has to be implemented with adequate structure, rules and processes. This concept is closely related to corporate responsibility regulation, and with due diligence concept. This means that executive board has to continually assess and analyze risks that enterprise faces in order to protect employees, investors, and clients from potential loses due to inappropriate business risks [10].

The difference of IS governance comparing to ISMS is that security is completely integrated and it is the part of business goals of the organisation.

b. Systemic Security Management Model

Systemic security management model (Fig.4.) includes into IS management approach additional element of organization (design/strategy), comparing to the traditionally used elements of people, processes, and technology. Besides that, the model includes dynamic interconnections among these four elements [18] [19]. The systemic security management model basically represents the use of the system theory, and comprehensive approach to information security on the highest organisational level, with a view to control information security based on the parameters that stem from the overall business goals.

The most important novelty of this model is clear expression of the viewpoint that security is consisted of dynamically interconnected multidimensional activities, in comparison to the traditional approach that used to treat information security areas separately and independently one from another.

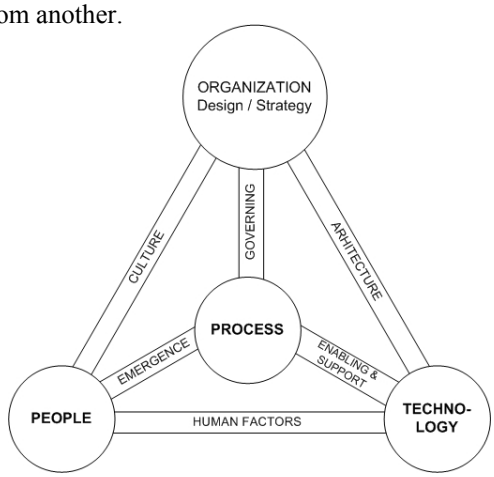

Fig.4. Systemic Security Management Model

c. Critical Information Infrastructure Protection

Methodology that is proposed in [17] formalize and quantifies the approach to critical infrastructure, explains the similarity of structures in different critical infrastructure sectors, and propose a few quantitative methods for the evaluation of vulnerability and for the establishment of optimal policies to reduce vulnerabilities.

The methodology starts with the claim that each infrastructure can be represented by the network of nodes mutually linked with connections. Simply by counting the number of connections per node the critical nodes (hubes) can be identified. Vulnerability and risk assessments are carried out with the use of Model-Based Vulnerability Analyses (MBVA). Within a framework of MBVA methodology the simple model of critical components in network is built, where the network analysis is combined with modelling of the fault tree, to derive vulnerability, risk, and the allocation strategy of protection resources. Complex networks of scale-free network type [37] do not have natural scale but some nodes have the scale of an order of magnitude bigger than the average node, and these nodes are cold hubs. Scale-free networks are exceptionally robust to accidental attacks on nodes, but they are very perceptible to targeted attacks on hubs that can fragment the network easily.

D. Security Metrics

Metric is generally the system or standard of measurement that is expected properties such as consistency, simple acquisition of data, quantitative expressions and the use of measurement units [13]. Security metrics imply the analysis and the interpretation of measured data in order to conclude on corrective actions.

In most organisations the only ways of acquiring information on security posture, are either through the risk management process or through some kind of audit or oversight. In doing so, the focus of risk management is not on the performance or strategic connection of security with business goals, but on the identification of possible risks to information assets and on the implementation of security controls. It is the operational level, sometimes tactical level, and very rarely the strategic level in the sense of business management. Added problem is the subjectivity in the risk management methodologies. On the other hand, the audit process assures mostly historical information regarding compliance issues, and can hardly be used for strategic management and assessment of trends, important for the management of the organisation in whole.

Metrics can be divided into several ways, such as the division according to what is measured (process, performance, results, quality, trends …), according to how it is measured (maturity process, balanced scorecard, evaluation, statistical analysis …), or based on the measured values (quantitative, qualitative and hybrid) [7].

a. Examples of Some Quantitative Metrics

Quantitative metrics is mostly technical metric or it is derived from IT and associated with performances and vulnerabilities. Usually performance measurements are divided as technical and non-technical.

Performance measurements of non-technical controls are related with maintenance and expenses. The return of investment (ROI) metric adapted to IS management is called return of security investment (ROSI). ROSI calculation is based on single loss expectancy (SLE) and annual loss expectancy (ALE), using asset value (AV), Exposure Factor (EF) and annual rate of occurrence (ARO). It is necessary to calculate the percentage of mitigated risk (%RM) and solutions cost (SC), in order to calculate ROSI (1).

$$ROSI = ((ALE * \%RM) - SC) / SC \quad (1)$$

The weaknesses of ROSI calculation are typical for risk management methodologies – assessment subjectivity of the key values: AV, EF, ARO, %RM …

The Fault Tree Analysis (FTA) is the methodology which uses graphical tool to show all possible faults of a complex system, from components to simple logic combination of components fault. The basic assumptions are that components fail accidentally, but according to the well characterised statistics, and that component faults on the lowest level of the tree are independent.

The certainty factor (CF) makes possible an expert evaluation of reliability of conclusions based on the expressions of belief and doubt in hypothesis and usage of different sources of answering to specific questions [7].

b. Examples of Some Qualitative Metrics

Qualitative metrics are typical for measuring quality of the processes, maturity of the operations and activities, or multidimensional approach with balanced scorecard, and they are very useful for management activities.

Cultural theory follows personal characteristics (viewpoint) through the division on typical ways of behaviour. In that way the theory can be applied to risk management and it can be useful in the activities of candidate selection for different security activities. In a similar way, the competing values framework is based on empirical studies of organisational effectiveness, where two dimensions of effectiveness are observed. One dimension is from internal focusing on persons towards external focusing on organization. The other dimension represents contrast between stability and management, and flexibility and changes of the organization. This method allows the setting of correlation between the organisational model and security potentials, for example in the risk management approach.

Capability maturity model represents the metrics of process maturity and it describes five process maturity levels: Initial, Repeatable, Defined, Managed, and Optimizing. Although very descriptive and simple to use, capability maturity model represents subjective assessment.

Balanced scorecard is basically hybrid metrics that combine quantitative and qualitative metrics into a multidimensional approach. It is based on four views: financial, users, internal business rules, growth and learning. The methodology converts mission and strategy of organization into a comprehensive set of measured performances that assure the framework for strategic measurement and control of the system. Performance measurement, based on strategy, assure the control loop for dynamic setting and improving of organisational strategy. Such approach creates strategically directed organisation.

V. CONCLUSION

The development of the field of information security management today is primarily directed towards multidimensional perception of information security policy. Such approach implies interconnection of different fields or domains of the information security policy, but also the relationship of this policy with corporate governance level.

Important direction of information security policy development is the incorporation of added factors that were not considered as security relevant in the traditional approach, such as organisational culture and structure. This leads to new areas or domains in information security policy.

The problem of subjectivity in the contemporary approach to the risk management is also one of the important development directions of the contemporary information security policy. The development of security metrics field and the approach to information security management through the information security governance as the part of overall corporate governance level, promises the decrease of subjective elements in future.

The field of policy and information security management research and development today is directed towards the information security strategy development within the framework of information security governance as the part of overall corporate governance [7] [14] [18] [19]. This direction gives answer to the economic justification of security investments, because these investments come directly from the business strategy and are measurable on that strategic level. Besides that, the comparison and evaluation of the security posture of different organisational entities, exists as the separate problem which is in research today, and requires the approach on the corporate level. Existing information security oversight methodologies are directed primarily towards the compliance against applied standard [3] [13], or prescribed security policy [2], but not in the direction of quantification and mutual comparison of the security posture in different organisations or state administrations.

REFERENCES

[1] Klaić, A., *Information Security Requirements in the Information Systems Planning Process*, 17th IIS Conference, FOI, Varaždin, 2006, p. 265-269

[2] Council Decision, *Adopting the Council's Security Regulations*, 19 March 2001, 2001/264/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:101:0001:0066:EN:PDF

[3] *HRN ISO/IEC 27001:2005, HRN ISO/IEC 17799:2005*, www.hzn.hr, www.iso.org

[4] Sherwood, J., Clark, A., Lynas, D., *Enterprise Security Architecture*, CMP Books, 2005

[5] Klaić, Aleksandar, *Information Security in Business and Government Sectors*, MIPRO 2005, Conference Proceedings BIS/DE/ISS, p. 193-198, Rijeka, 2005.

[6] *Zakon o tajnosti podataka i Zakon o informacijskoj sigurnosti* (NN 79/07)

[7] Brotby, W. Krag, *Information Security Management Metrics*, CRC Press, Auerbach, 2009

[8] Dunn, M., *A Comparative Analysis of Cybersecurity Initiatives Worldwide*, ITU, June 2005

[9] Tatalović, S., Grizold, A., Cvrtila, V., *Suvremene sigurnosne politike*, GM - Tehnička knjiga, Zagreb, 2008.

[10] Abele-Wigert, I., Dunn, M., *International CIIP Handbook 2006*, Center for Security Studies, ETH Zurich

[11] Peltier, T. R., *Information Security Policies and Procedures*, Auerbach Publications, 2004

[12] COBIT Mapping, *Overview of International IT Guidance*, IT Governance Institut, 2006, www.itgi.org

[13] Jaquith, A., *Security Metrics*, Addison-Wesley, 2007

[14] IT Governance Institute, *Information Security Governance*, 2nd Edition, 2006, www.itgi.org

[15] Newman, M., Barabasi, A. L., Watts, D. J., *The Structure and Dynamics of Networks*, Princeton University, 2006

[16] Anderson, R. J., *Security Engineering*, Wiley, 2001

[17] Lewis, T. G., *Critical Infrastructure Protection in Homeland Security*, Wiley-Interscience, 2006

[18] Kiely, L., Benzel, T., *Systemic Security Management*, Institute for Critical Information Infrastructure Protection (ICIIP), 2007

[19] ISACA, *An Introduction to the Business Model for Information Security*, 2009, www.isaca.org