Journal scientific and applied research, vol. 21, 2021
International Journal

Original Contribution

ISSN 1314-6289

POSSIBILITIES FOR ADAPTING SECURITY CULTURE MODEL AND ASSESSMENT TOOL FOR THE CORPORATE SECTOR

Vladimir Yankov

KOZLODUY NUCLEAR POWER PLANT, SECURITY DIVISION, 3321 KOZLODUY

E-mail: vladimir@vladoyankov.com

Abstract: *Each organization forms a unique organizational culture in accordance with the intentions and behavior of management, social and business environment in which it operates, the characteristics of employees, the presence of subcultures, etc. The characteristics of the organizational culture that are relevant to security form the security culture in that organization. It is important to implement security culture model and assessment tools for proper management of the human factors involved in security. This article explores the possibilities to adapt the existing models of security culture and the tools for its assessment for the needs of corporate sector.*

Keywords: *security, culture, human factor*

Due to the importance of the corporate sector for the national security, threats to the security of the companies largely follow global trends, including threats of radicalization, terrorist acts, organized crime and cyberterrorism. Preventing and neutralizing these threats only through security units, corporate and information security is becoming increasingly difficult in terms of the growing hybridity of these threats worldwide, and most companies still define security as primarily a technical issue.

Counteracting such complex and even as yet unforeseen threats requires certain values and attitudes shared by all in the companies, which determine the approach and understanding of managers and employees to security. These values and attitudes form the security culture as part of the organizational culture in the companies.

Each company forms a unique organizational culture in accordance with the intentions and behavior of management, social and business environment in which it operates, the characteristics of employees, the presence of subcultures, etc. It is now unequivocally proven and recognized that organizational culture is a significant factor in work, productivity, safety, compliance and staff discipline.

For these reasons, several methodologies have been developed to both assess and track the development of organizational culture over time.

The characteristics of the organizational culture that are relevant to security and form the security culture in the corporate sector have been partially studied, mainly in the field of information security. An overview of the existing models for security culture shows that there is no developed comprehensive model and assessment tool for security culture in the corporate sphere. Usually a distinction is made between information security and physical security, and the models and frameworks for information security culture (often mistakenly described only as security culture) are much better studied and developed.

The most comprehensive model and assessment tool for security culture was developed in the nuclear field. The International Atomic Energy Agency in 2008 developed a model of nuclear security culture based on Edgar Shine's model of organizational culture, which was successfully used in the 1990s to develop a model of nuclear safety culture.

Schein proposes that culture in organizations can be considered in layers comprised of underlying assumptions, espoused values and artifacts. Some layers are directly observable, while others are invisible and have to be deduced from what can be observed in the organization. Artifacts are the visible elements in a culture and include any tangible, overt or verbally identifiable elements in any organization. Espoused values are the organization's stated values and rules of behavior. Shared basic assumptions are the deeply embedded, taken-for-granted behaviours which are usually unconscious, but constitute the essence of culture.[1]

Using Edgar Schein’s three layers of culture, the IAEA model for nuclear security culture breaks the artifacts of the culture into three parts, giving a total of five elements (see Figure 1). They are beliefs and attitudes (corresponding to Schein’s “underlying assumptions”); principles for guiding decisions and behavior (corresponding to Schein’s “espoused values”); management systems, leadership and personnel behavior (corresponding to Schein’s “artifacts”). [2]

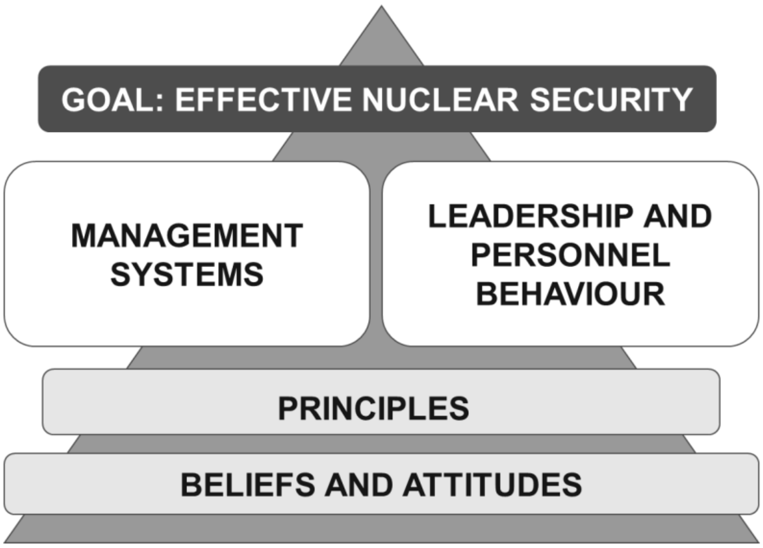
GOAL: EFFECTIVE NUCLEAR SECURITY
MANAGEMENT SYSTEMS
LEADERSHIP AND PERSONNEL BEHAVIOUR
PRINCIPLES
BELIEFS AND ATTITUDES

Fig. 1 IAEA Model of Nuclear Security Culture

The model is widely applicable to a wide range of nuclear facilities and organizations and since the majority of the models and frameworks for information security culture are also based on Schein's model of organizational culture, it can be concluded that this model will be applicable to the corporate sector as well.

To measure and assess information security culture have been developed different measurement instruments mostly based on surveys, which makes them tools for gathering quantitative data. The importance and complexity of the corporate sector, however, requires a more in-depth study of the security culture, which requires the use of combination of quantitative and qualitative data collection tools.

To support stakeholders in their efforts to gain a clear idea of the impact of the human factor on the security regime, IAEA developed in 2017 methodology for self-assessment of nuclear security culture. The methodology describes a multistage process comprising four different tools for collecting quantitative and qualitative data – survey, interviews, document review and observations. [3]

The effectiveness of these tools have been verified in three countries and at three different facilities: Indonesia's research reactors, Bulgaria's nuclear power plant, and at a hospital with radioactive sources in Malaysia. This means that these tools can be widely applied in the corporate sector as well. Depending on the field of activity and the desired scope of the assessment, at least a survey and interviews can be applied, which will provide quantitative input from a large number of employees and a source of qualitative data.

The IAEA nuclear security culture model and the self-assessment methodology are based on 30 characteristics of management systems and leadership and personnel behaviors. These characteristics are evaluated by comparing the current state of the culture to its optimal parameters specified by culture indicators. More than 300 performance indicators assigned to the characteristics were identified, which are not prescriptive, but serve as a base for further examination. An overview of the indicators shows that just a very small part of these indicators are nuclear specific. Most of them are universal and can be adapted for the corporate sector. Because of the complexity of the corporate sector, for instance, chemical companies are more vulnerable to terrorism, while in the financial sector a theft is more likely, it is not recommended sector-specific indicators to be included in assessment tool. Instead, the organizations can be encouraged to develop their own specific indicators during the process of assessment.

In conclusion, it can be said that Edgar Schein's model of organizational culture can be adapted for the corporate sector, and a general assessment method can be developed which to include quantitative and qualitative data collection tools and to encourage the stakeholders to supplement sector-specific means for more precise examination of the security culture in the different companies.

[1]. Schein, Edgar. The Corporate Culture and Leadership, 3rd ed. (San Francisco, CA: Jossey-Bass, 2004)

[2]. International Atomic Energy Agency, "Nuclear Security Culture: Implementing Guide," IAEA Nuclear Security Series No. 7, IAEA, Vienna, 2008

[3]. International Atomic Energy Agency, "Self-Assessment of Nuclear Security Culture in Facilities and Activities," IAEA Nuclear Security Series No. 28-T, IAEA, Vienna, 2018