Information & Security

E. Pavlova,
vol. 46, no. 3 (2020): 239-249
https://doi.org/10.11610/isij.4617

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation

Elitsa Pavlova

University of National and World Economy, Sofia, Bulgaria, http://www.unwe.bg/en

ABSTRACT:

The digital transformation (digitalisation) becomes an important item in strategies and plans for development and improvement of higher education. The implementation of new approaches in education, new ways of information sharing and group work are expected to improve and transform all processes and services within the higher education institutions. The digital transformation should not underestimate the security aspects of ICT use and specific Cyber Security Culture (CSC), part of the wider organisational culture should be directed, shaped and supported. CSC of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they are manifested in people's behaviour with information technologies. The attitude towards security measures in academic organisations is usually oriented towards free and open sharing of information and knowledge. This positive direction has to be maintained and preserved, but also to be changed and adapted to current threats and security environment. The balance between openness and security has to be analysed, rationally implemented, and monitored through establishment of organisational programme dedicated to CSC as a measure to influence the human factor in cybersecurity.

This article presents best practices of universities' digitalisation from the cyber security and CRC point of view. ENISA's CSC development guidance was used as the main tool for developing the general CSC programme for universities. The required changes of CSC and possible programme implementation are considered based on cases from several Bulgarian universities.

ARTICLE INFO:

RECEIVED: 31 MAY 2020
REVISED: 21 JULY 2020
ONLINE: 03 SEP 2020

KEYWORDS:

organisational culture, cybersecurity culture, digital transformation, university

✉ Corresponding Author: Tel.: +359 889 89 67 27; E-mail: epavlova@unwe.bg

Introduction

The biggest problem with cybersecurity facing higher education institutions is that many in the sector do not fully understand risk, and therefore a key first step is to develop guidelines for assessing and measuring this risk as accurately as possible. To address the challenges of the human factor, it will also be important to raise awareness among teachers and staff. Measures to encourage the disclosure and sharing of information can also play an important role in enhancing cybersecurity, as well as standardized management methods and security policies, improved communication to overcome cultural differences and the implementation of technical solutions.

The pandemic COVID-19 has changed the world and education is one of the most affected sectors. Over the past months, teachers, students and staff have changed their work habits daily and studied the functionalities of various platforms for online training, exams and conference calls. Pressed by the circumstances, they sought solutions, expanded their IT knowledge and digital skills. Lecturing in an empty auditorium in front of a camera, remote communication and reworking the lectures into presentations are examples of this. The goal was for the school year to end successfully, and the cost was to reduce security. The lack of good organizational and security culture became apparent. Security assessment and risk analysis were performed only on servers and firewalls vulnerable to cyber-attacks. Public universities haven't a budget for organizational and information security, no formal data ranking programs, access control systems, incident response plans, or security training programs. Untrained employees are the easiest target for social investment and that is why the topic is so relevant.

Methods

A detailed review of the literature is made and the steps of the method for implementation of organizational culture of ENISA, the peculiarities of the higher education institutions in Bulgaria and their implementation in the universities are considered in detail. Interviews were conducted with system and network administrators from several universities in Bulgaria and the practices and procedures of work during the pandemic were discussed. An analysis of the activity of universities and the changes that occur during digitalization has been made.

1. Organizational culture

The concept of organizational culture [1] was introduced in the field of management and organizational research in the late 1970s and it began to attract considerable scientific attention in the early 1980s. Andrew Pettigrew [2] was the first to present the concept of organizational culture. He offers ideas for concepts and processes and describes organizational culture as a set of beliefs, identity, ritual and myth – a definition that is still widely used.

Deal and Kennedy [3] in 1983 proposed a model of culture based on four organizational prototypes. Subsequently, Schein[4] 1985, discusses the culture of the organization as basic beliefs, which are shared consistently among the

members of an organization. Schein was the first to emphasize the role of the leader as the creator and maintainer of culture in organizations. In her scholarly work, Smircich [5] explores the significance of the concept of culture for organizational analysis and proves that the concept of culture can undertake an analysis of the organization in several different directions. There is a possibility for diverse cultural events within an organization and each of them can be reinforced through different methods. Theoretical research methods in this field are diverse.

The above conceptualizations and approaches to understanding culture continue to underlie and influence contemporary cultural research as well as practical attempts to manage culture in organizations.

Organizational culture [6] is a system of shared assumptions, values, and beliefs that governs how people behave in organizations. Based on sociology, organizational scientists have suggested that each organization can develop and maintain a unique culture that provides guidelines and boundaries for the behavior of members of the organization. Organizational culture can significantly affect organizational performance and can be used as a resource to create a competitive advantage.

Regarding to the information security, choices about which values are priorities and about which types of organizational culture to be introduced in higher education institutions are related to the organizational structure and the different management roles. Despite, the culture that arises naturally in most organizations, the cultures often start with a process called "gradation of values." The organizational culture that is formed by management can be maintained through staff training, analysis of existing practices, and moral and material incentives, the achieving gradation of the values.

Through the development of organization culture, the positive attitude of employees to the management goals and requirements can be achieved.

2. Information and security culture

Psychology consider personal information culture as a kind of subsystem that provides the right level of the most important processes in life. These processes may include the following:[7]

- Knowledge generation;
- Effective exchange of information, which is provided by forming a set of information skills;
- Development and improvement of individual effective ways to store and absorb information;
- Information ethics, regulating access to someone else's information.

All these necessary processes and skills are part of the concept of information culture.

A CSC related research conducted by the University of Albany concluded “A leading cause of security breaches is a basic human vulnerability: our susceptibility to deception”.[8] With the increase in users connecting to cloud servers,

email, social media, and daily internet usage, the opportunity for breaches of a business network become higher, because of the human factor in the most vulnerable link of cybersecurity. Establishing a solid cyber defence requires the creation of a cybersecurity culture within the organization.

3. Cybersecurity Culture

Cybersecurity is defined by some authors as a set of policies, tools, concepts, guides, actions, training, good practices and technologies that can be used to protect cyberspace, organizations and consumers.[9]

ENISA defines the Cyber Security Culture (CSC) of organizations as "people's knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values regarding cybersecurity and how they manifest themselves in people's behaviour with the help of information technology." The document "Cyber Security Culture in organisations" recommends that the CSC be "an integral part of the employee's work, habits and behaviour, including them in his daily activities."

Currently, cybersecurity is the most pressing IT issue for many organizations – including higher education institutions.[10] The usual risks are compromised data, stolen research, and reputational damage.

Cyber security focus should be on communications and culture – not big funding or sophisticated technical systems. Increasing cyber security awareness and process knowledge through staff training programs is the surest way to effect sustained behavioural change.

To maintain their collaborative culture, colleges and universities implement robust information technology networks and multi-layered infrastructure systems with varying levels of access and connectivity.[11]

Unfortunately, this open environment made institutions of higher education (IHEs) worldwide in cyber-attacks in 2019 and reinforced the need for increased higher education for a culture of cybersecurity. The security challenge must be tackled collectively – by management, IT staff, academic staff, and students. The education sector must protect its networks and resources from unauthorized access and cyber threats, and the implementation of ENISA guidelines can be successfully applied to this end.

Achieving a strong cybersecurity culture requires actions on people, processes, and technology. An effective risk management program is the foundation of a good culture of cybersecurity. Assessing and understanding the safety and security culture of the organization can lead to an understanding of how safety and security effectiveness can be maintained, as well as to identify vulnerabilities that can lead to downtime and be the reason for failure.

Changes in universities' activities during digital transformation in higher education are presented in Table 1.

Table 1 shows the changes that occur in universities during the digital transformation in various activities – training, research, e-mail, organization, management. They are chosen in order of importance and are an integral part of life at any university. These activities are related to confidential information, account and password management and depend on the level of organizational

Table 1. Universities' activities, real-world and digital changes.

Activity	Real-world changes	Digital changes
Education, study programs	new skills, new knowledge, new teaching styles	decentralized digital solutions for faculties, implementation of digital educational resources, ensuring continuity and incessancy of learning
Research	traditional research methods	creating or developing digital solutions
E-mails and notifications	5-10 per day	20-60 per day
Organization	re-organized processes, flatter hierarchies, decentralization	web-based and data-based work processes and collaboration, paper-to-digital solutions, decentralized digital administration
Management	formation of organizational and information culture	formation of organisation, security and cybersecurity culture
Role in society	higher demand for innovation transfer	higher demand for innovation transfer platforms, social media

culture. They are usually part of the goals and mission of the university. Management must form an organization, a culture of security and cybersecurity, innovation and digital solutions that are well thought out and reasoned to help all stakeholders.

University Cybersecurity Culture Enhancement through ENISA Guidelines

By analysing ENISA's methodology and security culture in higher education, new guidelines can be developed to meet the needs and characteristics of higher education institutions. An implementation of ENISA's process for CSC programs covers the creation and implementation of CSC programs in the form of a step-by-step implementation framework focused on specific activities, their implementation, and measurement of impact.[12] The approach is iterative, as after each CS activity the impact is measured, the results are reviewed and the approach is reviewed. New activities can then be selected or delivery methods can be changed. This also makes it possible to review and modify the initial goals

and/ or target audience. While each organisation may need to modify the Implementation Framework to meet the unique needs of its context, such modifications should be undertaken with care.

Safety culture is very difficult to measure directly and such measurement can be obtained, for example, through direct observations or interviews. The methodology borrows tools from the social sciences for its implementation; in particular, it is based on questionnaires, interviews, on-site observations, and self-assessment.

Developing and implementing a successful CSC program based on ENISA recommendations for higher education is a task that requires a multileveled approach. It must take into account the complex organizational structure of universities and serve their specific needs.

Higher education institutions are large and complex organizations with a hierarchical structure at three levels: university management, faculties, and departments. The large-sized university has nearly 20,000 students and 1,000 faculty and staff. The wide age range of participants (18-65 years), the presence of many national cultures, different levels of IT competence, the large number of computers, and the complex network connectivity of all devices make the creation and management of CSC extremely difficult. The ENISA guide states that "If CSC programs and activities become too burdensome, there is a risk that employees will resist or ignore the application of CS messages, technologies and practices. The CSC should be formed with employees, not imposed on them."

Digital transformation separates the main processes and assembles them in a new and more efficient way. Higher education is a sector that has unique organizational models, processes and goals. From the analysis of key activities, the educational process includes planning, coordinating courses, teaching, student learning, tracking, student performance, and indicators. The research process covers specific activities such as setting objectives, funding applications, identifying partners, conducting research, enhancing the impact on research, reviewing results and publishing. In addition to these basic processes, there are supporting processes such as authorization, planning and management.

The following figure illustrates the complexity of planning processes in higher education based on the analysis of activities.

The implementation framework that ENISA provides components for creating and measuring the success of CSC programs contains eight steps that are selected and combined by the internal CSC implementation team. Redesigned for the specific needs of universities, it looks like this:

Step 1: Create a basic CSC workgroup. The working group should include deans of faculties, heads of departments, cybersecurity experts, as well as representatives of the academic community, why they have the best view of the work in these organizational units. Consideration should be given to how the CSC functionalities will be distributed among them.

Step 2: Structuring activities and risk assessment. A key element of this process is the mapping and evaluation of current / future security measures. Much of the workplace action is related to cyberspace, access to local databases, and

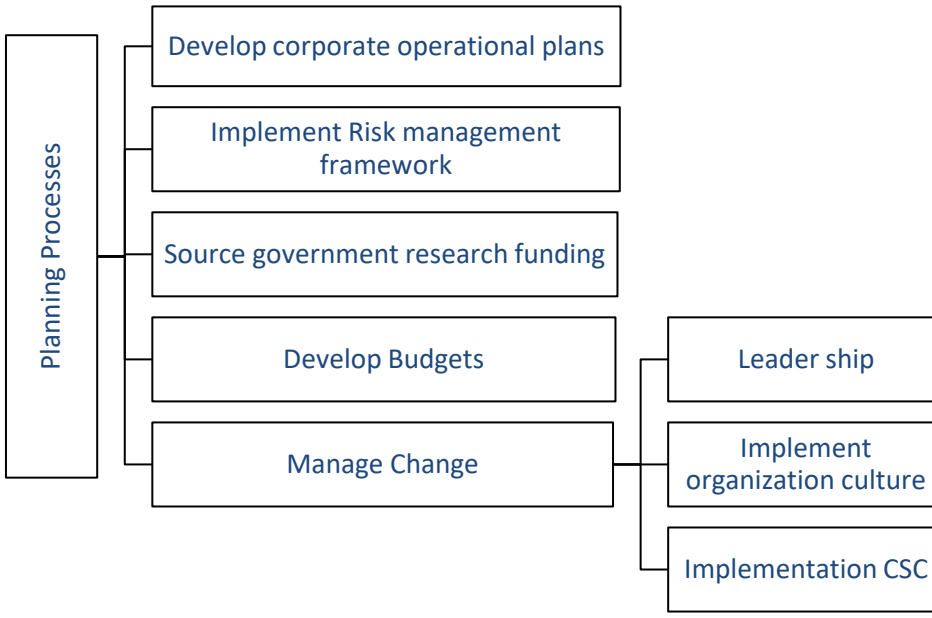

Figure 1: Planning processes in higher education.

programs. Teachers and staff prefer to work with easy passwords that keep in their browser, quick links to the desktop, and do not consider it necessary to close work sessions at the end of the day. They do not feel threatened by cyberattacks and believe that the university's IT department has taken care of everything. Identifying trade-offs and conflicts are important for the success or failure of a future CSC program. If employees are put in a position to be unable to do their jobs without violating cybersecurity policies, then the CSC at this university will become inapplicable.

Step 3: Defining the main goals, success criteria and the target audience.

Step 4: Review the current situation and analyse the difference between the current situation and the set goals. Increase information security through employee training – organization culture, Windows sharing, local security policy, password management.

Step 5: Selection of activities. A large number of activities and services offered by the university, as well as the limited resources at its disposal, must be taken into account.

Step 6: Choosing a method for performing the activity/service in accordance with the university resources. Security vulnerability testing with free tools such as NetBIOS, Microsoft Baseline Security Analyzer.

Step 7: Measure the current situation and analyse the results. At the end of the activity/activities, the CSC measurement should be repeated and compared with the current situation and objectives (step 4) and the analysed results in

order to identify the levels of success and failure. Changing the CSC in an organization is an ongoing process.

Step 8: Review the results before deciding on the next action.

Figure 2 shows the ENISA approach applied to CSC processes in higher education.

Security policies are the first step in implementing an information security management system (ISMS) at the university. ISMS ensures continuous improvement of information security, taking into account the interests of stakeholders; confidence that modern information security requirements will meet by complying with relevant standards.

Security policies are approved by management and should include:

- Definition of information security, its purpose, scope, and significance;
- Management goals, implementation, and principles;
- Structure of the control environment, rules for risk assessment and management;
- A brief explanation of the need for this security policy and standards;
- Reporting.

Documents developing security policy at horizontal and vertical levels, such as detailed security policies and rules for specific information systems.

Building and enhancing the culture of cybersecurity in universities based on the ENISA approach, combined with well-developed information security policies, will help the digitalization of higher education in Bulgaria.

In the era of technology and global economic change, universities in Bulgaria need a comprehensive governance model for the digitalization of IT and the culture of cybersecurity, which already exists in many European educational systems. Examples of successful management approaches are the Norwegian University of Science and Technology, the University of Oslo, the University of Gothenburg, the Universities of Oxford, Cambridge and Bath in the United Kingdom. Organizational culture affects the quality of research, the reputation of the university, education and all its activities.

Bulgarian universities lag behind in international rankings and there are many areas that need to be improved. More than 50 universities from Bulgaria find a place in Webometrics. Sofia University “St. Kliment Ohridski” is on the first place in the ranking of the Bulgarian universities and on the 942nd place in the general ranking.

The number of students determines the size of the university and the complexity of IT management in it. The ranking data for the web pages show the place on the university's website, both globally (category: Education) and regionally.

The main criteria for these rankings are structures, content, usefulness and search, connectivity to social networks and platforms, number of visits, mobile applications, information updates and other parameters directly related to the organizational culture and quality of services provided.

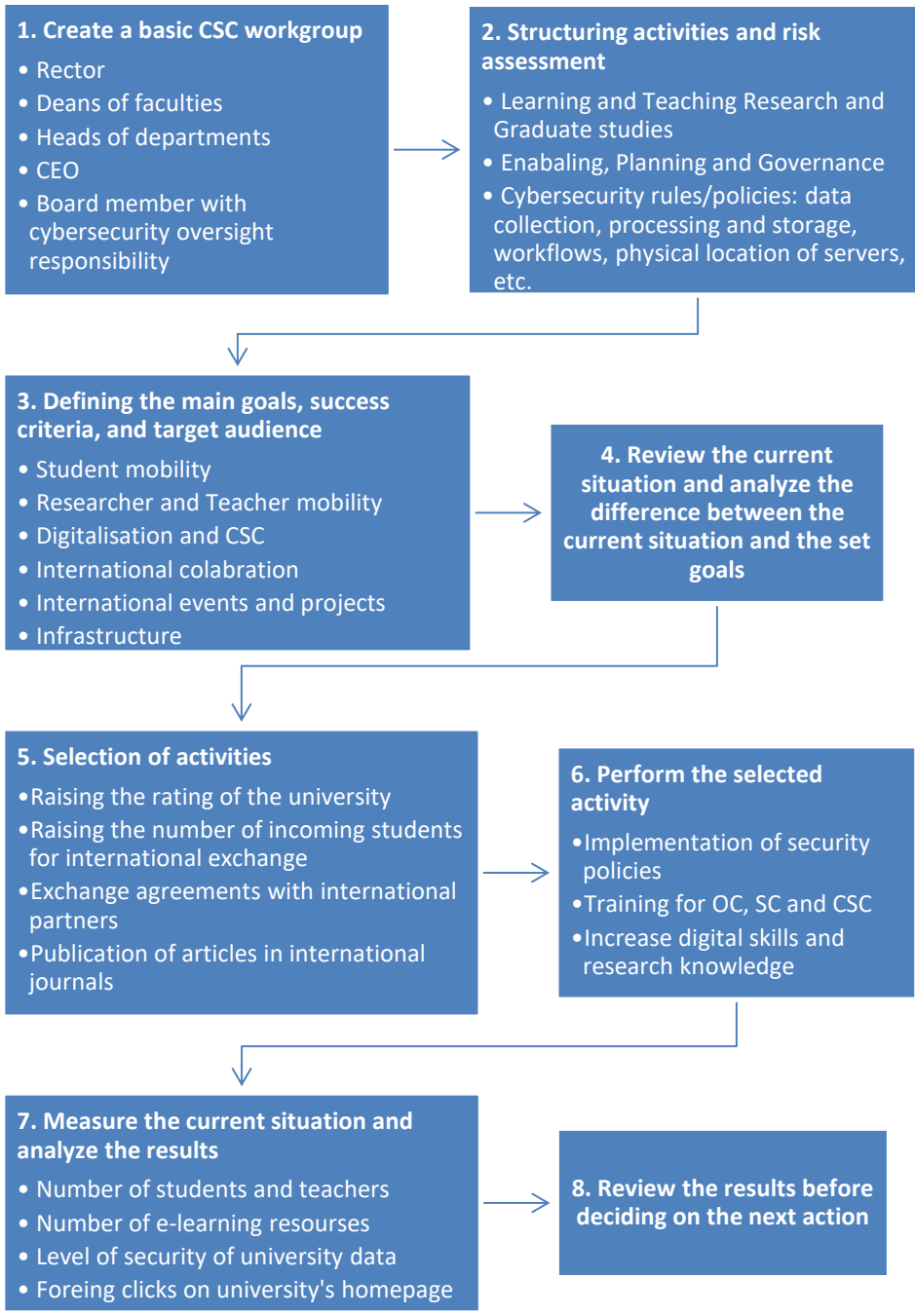

Figure 2: The implementation framework of CSC processes in higher education.

A review of the websites of the leading universities in Bulgaria shows that they do not publish a strategy for digitalization, security policies, provisions for organizational and information security.

Conclusions

This report examines ENISA's approach to organizational culture related to cybersecurity during the university's digital transformation.

The methods proposed in the report for raising the organizational culture based on the ENISA approach must lead to certain norms of behaviour and increase security in all activities of the university. The opposite statement is also true. Approaches to enhancing a culture of security should lead to increased trust in the university, reduced risk of cyberattacks and response time. Based on the created algorithm, programs for digital identity management, access to critical resources, organizational security and cybersecurity in higher education institutions can be prepared. Employee training is extremely important because the human factor is the weakest link in the security of any organization.

Acknowledgements

My sincere gratitude to my supervisor, Associate Professor Dr. G. Penchev, for providing guidance and feedback throughout this project.

References

[1] Oxford Bibliographies, “Organization Culture,” *Oxford Bibliographies*, November 14, 2018, https://www.oxfordbibliographies.com/view/document/obo-9780199846740/obo-9780199846740-0059.xml.

[2] Andrew M. Pettigrew, “On Studying Organizational Cultures,” *Administrative Science Quarterly* 24, no. 4 (1979): 570–81, https://doi.org/10.2307/2392363.

[3] Terrence E. Deal and Allan A. Kennedy, “Corporate Cultures: The Rites and Rituals of Corporate Life: Addison-Wesley, 1982,” *Business Horizons* 26, no. 2 (1983): 82–85.

[4] Edgar H. Schein, *Organizational Culture and Leadership* (John Wiley & Sons, 2010).

[5] Linda Smircich, “Concepts of Culture and Organizational Analysis,” *Administrative Science Quarterly* 28, no. 3 (1983): 339–58, https://doi.org/10.2307/2392246.

[6] “What Is Organizational Culture?” *Study.Com*, accessed June 11, 2020, https://study.com/academy/lesson/what-is-organizational-culture-definition-characteristics.html.

[7] Educause, “Information Security Guide,” *Educause*, September 13, 2019, www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources.

[8] Cytelligence, “Why You Need to Establish a Cyber Security Culture in Within Your Organization,” *Cytelligence*, March 20, 2018, https://cytelligence.com/why-you-need-to-establish-a-cyber-security-culture-in-within-your-organization/.

[9] Natalia G. Miloslavskaya, “Cybersecurity Culture as an Element of IT Professional Training,” *ResearchGate*, June 10, 2016, www.researchgate.net/publication/305870129_Cybersecurity_culture_as_an_element_of_IT_professional_training.

[10] Sony Michael, Karingada Therisa Kochu, and Baporikar Neeta, Quality Management Implementation in Higher Education: Practices, Models, and Case Studies (IGI Global, 2019).

[11] "Cybersecurity Considerations for Institutions of Higher Education," *Rems*, June 5, 2019, 11, https://rems.ed.gov/docs/Cybersecurity_Considerations_for_Higher_ed_Fact_Sheet_508C.pdf.

[12] ENISA, "Good Practice Guide on Training Methodologies," Report/Study, *ENISA Europa*, accessed June 7, 2020, https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies.

About the Author

Elitsa **Pavlova** is a doctoral student at the University of National and World Economy at the Department of National and Regional Security. The topic she is working on is "Development and Implementation of a Model for Digitalization Management of Higher Education Institutions in Bulgaria. Security Aspects." She graduated with a master's degree from the same department in 2006 and a master's degree in engineering at the Technical University in Sofia in 1999. She works as a network administrator in the Department of Information Technology at UNWE.