Trakia Journal of Sciences, Vol. 21, Suppl. 1, pp 591-5962023

Available online at:
http://www.uni-sz.bg
ISSN 1313-3551 (online) **doi:10.15547/tjs.2023.s.01.098**

MODERN ASPECTS IN THE DIGITALIZATION OF BUSINESS AND REGIONS

R. Kirilov*

Department of Informatics, Faculty of Applied Informatics and Statistics, University of National and World Economy, Sofia, Bulgaria

ABSTRACT
Purpose. The last few years have given a very strong impetus to the development of digitization in all spheres. This applies to business organizations, both nationally and regionally. The development aims to present some of the modern aspects of these processes. Attention is also paid to cybersecurity issues at the regional level. Methods. The methods used are related to: comparative analysis of the digitalization challenges; assessment of contemporary aspects and issues; inferring basic decisions and forming trends. Results. The main results are in the direction of defining the modern aspects in the digitalization of business and regions. Conclusions. The conclusions are in the direction of proposals for improvement in the digitization policy at the national and regional level.

Key words: Digitalization, Information technologies, Cybersecurity.

INTRODUCTION

Modern Bulgarian society in recent years is in a continuous process of digital transformation. This applies both to business organizations and to all representatives of central and local government. The expectations of businesses and citizens are for transparent service, clear processes, high efficiency and speed of service and modern digital administrative services.

The direction of development of digitization processes in the Republic of Bulgaria largely corresponds to the priorities set in the main European and national documents. Dynamics in the European strategic and regulatory framework have been intensifying in recent months. On 18 April 2023, the European Commission (EC) is proposing an EU Cyber Solidarity Act to strengthen cybersecurity capacity in the EU (1). A few days later, on April 25, 2023, the Digital Services Act (2) was formalized, with the commission specifying the first set of very large online platforms and search engines. On 4 May 2023, the commission adopted a recommendation on how to combat commercial-scale online piracy of sports and other live events. The development of strategic and normative documents at the European level also causes an expansion of project opportunities in the field of digitization in the public sector.

In 2021, the so-called Digital Decade policy program (3) is being developed, which defines several main priorities:

- Skills;
- Digital transformation of business;
- Secure and sustainable digital infrastructures;
- Digitization of public services.

All this shows the key importance of digitization processes for the development of modern organizations.

METHODS

The main concept in the present study is about the relationship between the digitization of organizations and maintaining the necessary level of cyber security. On the one hand, the expectations of citizens and businesses are for increasingly broad and large-scale digital services, which, however, should have a

***Correspondence to**: *Rosen Kirilov, Department of Informatics, Faculty of Applied Informatics and Statistics, University of National and World Economy, Sofia, Bulgaria, 1700 Sofia, Student District, UNWE, e-mail: rkirilov@unwe.bg, phone: +359 2 8195 451*

guaranteed level of security. In this regard, the application of a methodological toolkit in the research is aimed at analyzing some of the regional aspects of digitization related to:

- Defining the need for investments in technical and information infrastructure. Here, the main challenge is finding a balance between using your own server infrastructure and cloud infrastructure provided by data centers. It should be noted, that the presence of an additional layer in the architecture of the software solution leads to a certain improvement in security in terms of access to the information system's data (4).
- Defining the need to outsource processes and services to external companies and suppliers. Performing an analysis of the main challenges in this direction shows complexity in finding a balance between developing own digital services (5) or hiring ready-made solutions through outsourcing.
- Assessment of available human capital and specifically information technology professionals. The main challenge here is attracting and retaining professionals with the right knowledge, skills and competencies for IT support.

The literature contains several studies by leading authors on the issues of regional development and regional business. Based on these studies and research, the following priorities for the development of business and regions can be determined:

- Intelligent management of the urban environment (population, migration processes, etc.).
- Expanding the number and access to digital administrative services at the local level.
- Introduction of intelligent transport systems, using artificial intelligence.
- Waste management and ecosystems.
- Crisis and disaster management, through big data analysis, etc.

The main method used in the present study is an analysis of the level of cyber security ensured in the organization. National legislation in this area has been very strongly developed in recent years.

A serious challenge for any modern organization is the provision of cyber security measures. The NIS Directive (6) was introduced into European legislation in 2016 **(Figure 1).**

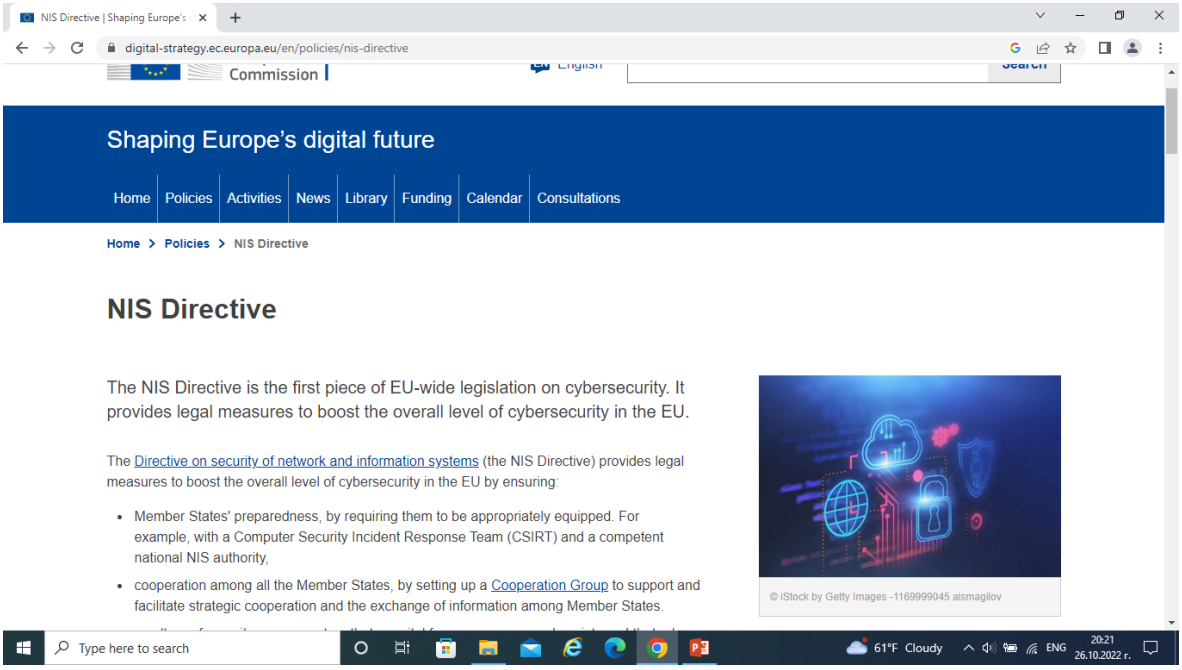

Figure 1. NIS Directive

In the national legislation, the NIS Directive has been transposed into the REGULATION on the minimum requirements for network and information security Adopted by PMS No. 186 of 26.07.2019, promulgated, SG, no. 59 of 26.07.2019, in force from 26.07.2019. According to the current provisions of this directive and the adopted ordinance, municipalities and higher education institutions fall within its scope.

In 2022, the European Commission adopted an advanced version of the cyber security directive, under the name NIS2 (7) **(Figure 2).**

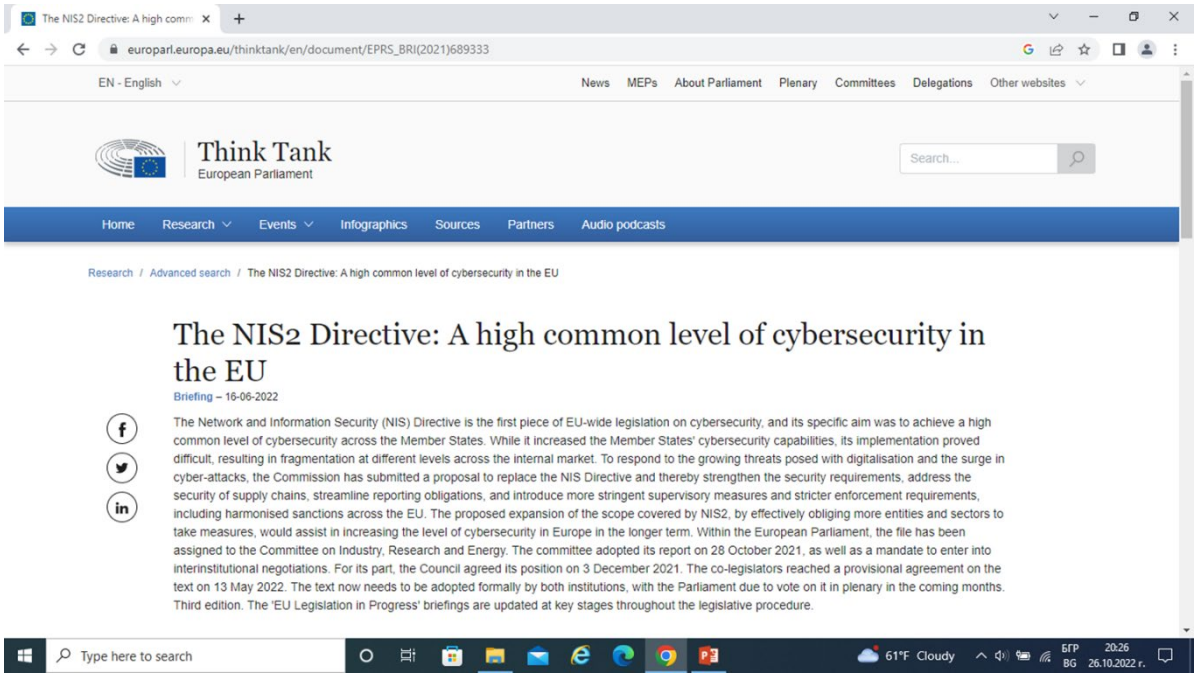

Figure 2. NIS2 Directive

The directive sets much higher requirements for network and information security. At the same time, the scope of application of security measures is being expanded. In the coming months, this European legislation will be transposed into the national one. Public organizations and private sector companies should provide additional measures to increase the level of cyber security of their own assets.

RESULTS

The study of digitization processes in business and regions gives reasons to believe that it is necessary to build a comprehensive model for cyber security of organizations. This is a very complex and responsible task, and in each specific case the conceptual framework should be different. It must accurately and clearly reflect the specifics of the organization and the specific features of business processes.

Within the framework of the present study, we propose a variant of a similar conceptual framework for ensuring a level of cyber security in a public organization **(Figure 3).**

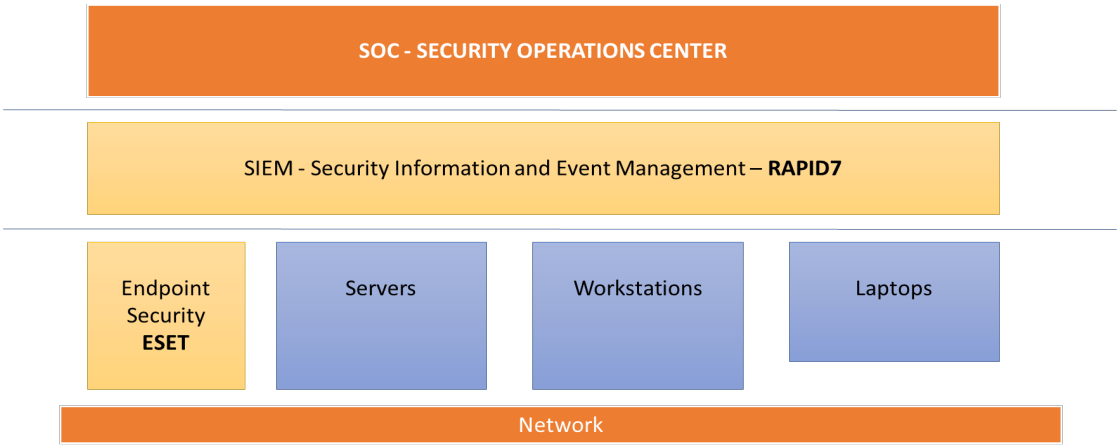

Figure 3. Conceptual Model for Cyber Security

The model consists of three layers. At the first layer are the specific computer configurations, servers, laptops, and network infrastructure. To make it possible to observe, monitor and administer, it is necessary to install software agents. For the model presented, ESET was selected as Endpoint Security software. The reasons for this are in a 2019 Gartner study, which classified this type of software in the group with a higher market rating and user choice (8) **(Figure 4).**

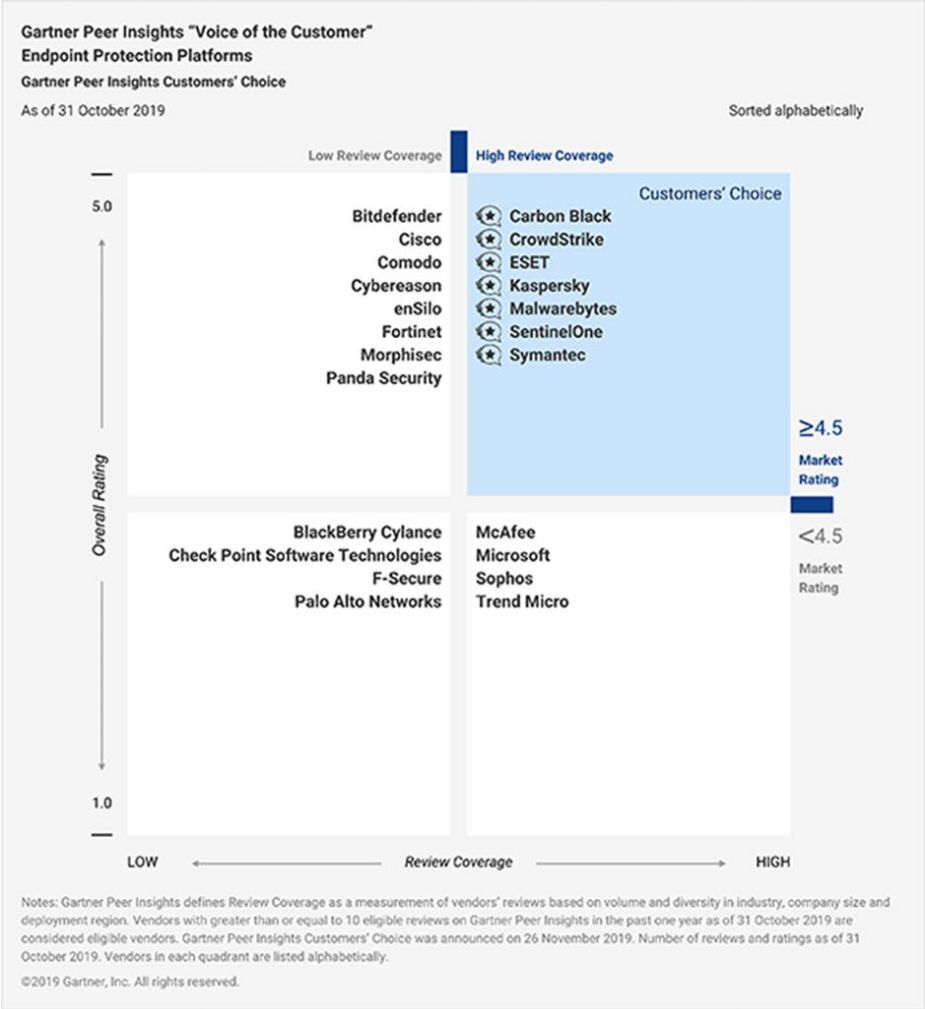

Figure 4. ESET Market Rating

As Endpoint protection software, ESET also offers very good opportunities for managing computer assets in the organization, as well as monitoring the status of each of the machines **(Figure 5).**

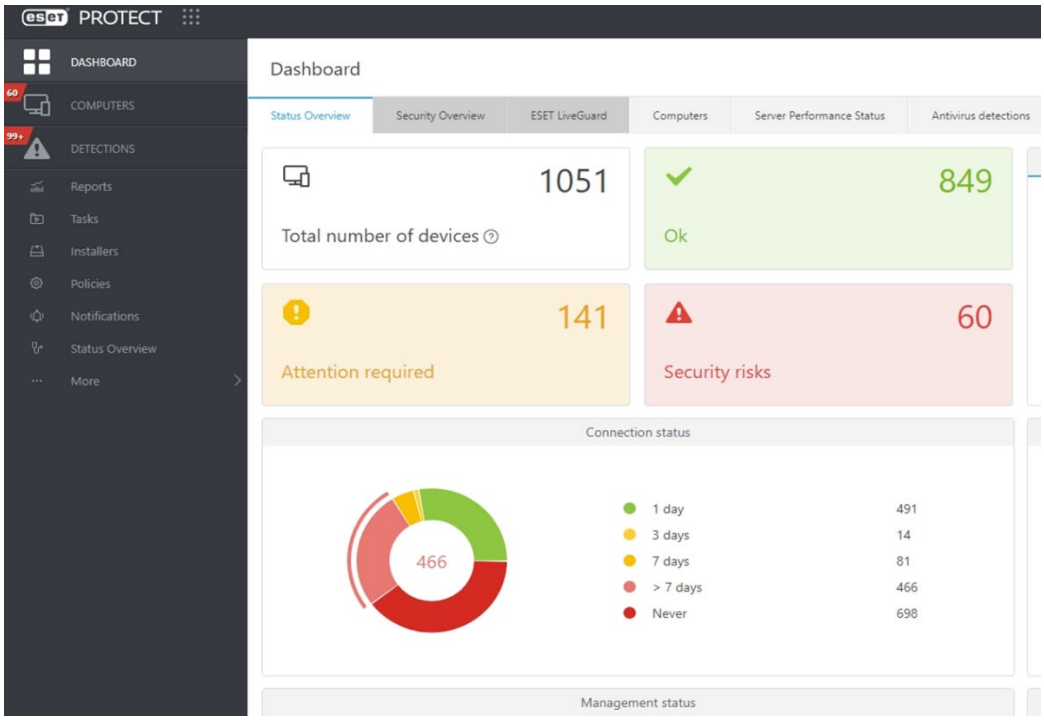

Figure 5. Asset management with ESET

On the second layer, the software agents of the first layer (ESET) report all possible incidents, logs, specifics in a specific cloud environment. In the specific model, the Rapid7 environment was chosen, which, by analogy with ESET, has a high market rating, according to Gartner (9) **(Figure 6).**

Figure 6. Rapid7 Market Rating

On the third layer of the proposed conceptual model is the Security Operational Center. In it, based on the aggregated data about the information infrastructure received in Rapid7, conclusions are drawn, and knowledge is formed using AI algorithms. They help identify various incidents with the infrastructure and applications within it, as well as proactively manage the organization's cybersecurity.

CONCLUSION

In conclusion of the present study, it is important to emphasize that digitalization processes in public and business organizations are continuous. They give rise to the need for several changes in business processes and ways of working. At the same time, digitization and the introduction of new digital administrative services significantly increases work efficiency and satisfaction for citizens and businesses. This should be a leading motive in access management and administrative service.

In the present study, an attempt is made to outline the conceptual prerequisites for the introduction of modern cyber security management models in large organizations. This process is considered in three of the broadest aspects, namely: technical, software and organizational aspects. Practical examples show that these three dimensions of cyber security should be implemented simultaneously and work in sync. Investments in technical infrastructure cannot bring the necessary effect if there is a lag in the other two dimensions and vice versa.

The practical results of the present study can provide direction for deepening research in the field of digitization and cyber security, as well

as provide valuable guidance for improving core processes.

REFERENCES

1. https://digitalstrategy.ec.europa.eu/bg/policies/cyber-solidarity
2. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_bg
3. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
4. Milev, P., Integration of Software Solutions via an Intermediary Web Service, Trakia Journal of Sciences, 17 (1), p. 181-185, 2019.
5. Kirilova, K., Naydenov, A., Development of Digital Administrative Services in the Republic of Bulgaria, Economic and Social Alternatives, 4, p. 5-17, 2022.
6. https://digitalstrategy.ec.europa.eu/en/policies
7. https://digitalstrategy.ec.europa.eu/en/policies/nis2-directive
8. https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/eset/product/eset-protect
9. https://www.gartner.com/reviews/market/application-security-testing/vendor/rapid7