ON RELATIONS BETWEEN CYBER SECURITY INDEX AND ISO 27001 STANDARD INDEX IN WESTERN BALKAN COUNTRIES

Enriko Ceko

Business Administration and Information Technology Department, Faculty of Economy, Canadian Institute of Technology, enriko.ceko@cit.edu.al , ORCID: 0000-0002-3372-2785

Abstract:
My aim in this article was to illustrate the relationships between the Western Balkan nations' ISO 27001 index and the cyber security index, given the growing global interest in cyber security.
The primary findings of this study were derived from the research methodology, which involved gathering data and information about the degree of cyber security applications in the Western Balkans, as represented by the cyber security index, as well as data about the degree of ISO 27001 standard application in Western Balkan countries, processing data for ISO 27001 certificates, creating an index of ISO 27001 certificates, and managing a regressive analysis on the relationships between the cyber security index and the ISO 27001 certificates index, while examining the path toward EU integration, they are also working to address concerns related to cyber security. This is because gaining a competitive edge in fields like information technology, artificial intelligence, digitalization, e-commerce, and e-government necessitates robust cyber defenses.
The primary suggestion is that Western Balkan nations may better respond to cyberattacks and cyberthreats by implementing ISO standards including the ISO 27000 family of standards, particularly ISO 27001.

Keywords: Cyber security index, ISO 27001 index, Western Balkans, information technology management, competitive advantage.

1. Introduction

Cybersecurity is the process of defending networks, sensitive data, and electronic devices from hostile assaults. 2023; Kaspersky). It is often referred to as electronic information security or information technology security.
Network security, application security, information security, operational security, disaster recovery and business continuity, and end-user education are some of the areas into which cybersecurity may be subdivided.
Network security is the process of protecting a computer network from outside threats, such as malicious viruses or targeted attackers. The goal of application security is to prevent threats from entering devices and software.
Data integrity and privacy are safeguarded during storage and transmission using information security measures.
The procedures and choices made for managing and safeguarding digital assets are part of operational security.
Disaster recovery and business continuity pertain to an organization's response to an event that results in the loss of operations or data, such as a cyber-security incident. End-user education targets the most erratic aspect of cyber-security: human behavior.

There is an increasing number of data breaches every year, and the global cyber threat is still evolving at a rapid rate. Global investment in cybersecurity solutions is inevitably rising as the danger posed by cyberspace is expected to continue growing in scope.

According to Gartner, investment in cybersecurity will top $260 billion worldwide by 2026 and reach $188.3 billion in 2023.
An international live index that gauges a nation's readiness to stop cyberattacks and handle cyber events is called the National Cyber Security Index.
In addition, the NCSI serves as a tool for developing national cyber security competence and a database including publicly accessible evidentiary materials (NCSI, 2023). NCSI assists with the following tasks:
- Determining the primary cyber threats
- Determining the security measures and capacities
- Choosing significant and quantifiable components
- Developing cyber security indicators
- Classifying cyber security indicators

Controls are unquestionably necessary to ensure the security of devices, communication networks, and information assets given the increasing number of security events and assaults on information and IT systems that enterprises are facing.

*Corresponding author:

The idea of cybersecurity was born out of this requirement. Attacks of this kind try to gain access to, alter, or remove private data that belongs to companies. Adopting strong cybersecurity measures is a difficult task as hackers are always coming up with new ways to launch attacks thanks to the abundance of tools and technology available. Nonetheless, there is a method for putting data and information security measures into place that partly simplifies and normalizes the process of putting these IT security measures into place.

In the current market, businesses want to give their clients trust and show that they are dedicated to protecting the security of the data they handle.

To do this, a firm might gain a competitive edge by obtaining certification of an ISO standard or security regulation, which attests to the proper management of security needs in information processing operations.

These are the information security and cybersecurity-related ISO standards and rules. The International Standards Organization creates and disseminates ISO standards (ISO). The ISO 27000 series of standards is one of them. This group of information security standards lays out the conditions and recommendations for putting in place an Information Security Management System (ISMS) to handle information security inside a company.

The primary standard in this group is ISO 27001, which serves as the series benchmark. The criteria for creating, implementing, maintaining, and continuously improving an ISMS are outlined in this standard.

The private sector is the primary implementer of ISO standards, but public administration bodies are also involved in cyber security matters. Therefore, for a nation to be safe from cyberattacks, there needs to be a strong correlation between government cybersecurity initiatives and the implementation of ISO 27001 standards.

2. Literature review

2.1 The Western Balkans as a part of the Balkan region

The Balkans, which roughly correlate to the Balkan Peninsula, are a region in southeast Europe that has been defined in a variety of ways throughout history (Gray & Sloan, 2014). The Balkan Mountains, which encircle all of Bulgaria, gave rise to the region's name. The Black Sea borders the northeast of the Balkan Peninsula, the Adriatic Sea borders the northwest, the Ionian Sea borders the southwest, the Aegean Sea borders the south, and the Straits forms the east.

There are many definitions for the peninsula's northern boundary (Vezenkov, 2017). Musala, located in Bulgaria's Rila mountain range at 2,925 meters (9,596 feet), is the highest peak in the Balkans.

German geographer August Zeune, who thought the Balkan Mountains were the main mountain range in Southeast Europe, stretching from the Adriatic Sea to the Black Sea, invented the idea of the Balkan Peninsula in 1808 (Todorova, 1997). In the 19th century, the regions of Europe that were then provinces of the Ottoman Empire were referred to as Rumelia or the Balkan Peninsula.

Its definition was more geopolitical than geographical, and it was furthered by the early 20th-century establishment of the Kingdom of Yugoslavia. Since the technical definition of a peninsula differs from the concept of the Balkan Peninsula's natural limits, contemporary geographers reject the notion of a Balkan Peninsula, while historical researchers typically discuss the Balkans as a region. Due to several conflicting definitions, the boundaries of the Balkans are up for debate. Regarding the region's constituent parts, there is no unanimous consensus. According to most definitions, the phrase includes all of the following: North Macedonia, Albania, Kosovo, Montenegro, Bulgaria, Greece, Bosnia and Herzegovina, and a sizable portion of Croatia and Serbia. The phrase is occasionally used to refer to Romania and the southern regions of Slovenia.

Italy is usually omitted, even though according to certain definitions it has a minor portion of its land on the Peninsula.

The economies of Albania, Bosnia & Herzegovina, Kosovo, Montenegro, the North Macedonian Republic, and Serbia are together referred to as the Western Balkans, which comprise the Balkan area, all looking towards EU integration, specifically discussing with the EU standards, cyber security, and ISO standards issues included.

Table 1. Western Balkan Countries General Data

	Albania	Bosnia and Herzegovina	Kosovo	Montenegro	North Macedonia	Serbia
Population	2,862,427	3,502,550	1,795,666	622,182	2,077,132	6,963,764
Area km²	28,749	51,197	10,908	13,812	25,713	77,474
Density 100/km²	100	69	159	45	81	91
Water area (%)	0.047	0.0002	0.01	0.0261	0.0109	0.0013
GDP nominal bln	$15.418	$20.106	$8.402	$5.424	$12.672	$55.437
GDP PPP, bln	$38.305	$47.590	$20.912	$11.940	$32.638	$122.740
GDP/head nominal	$5,373	$5,742	$4,649	$8,704	$6,096	$7,992
GDP/head	$13,327	$13,583	$11,664	$19,172	$15,715	$17,552
Gini Index	29.0	33.0	29.0	36.7	31.9	35.6
HDI	0.791	0.769	0.739	0.816	0.759	0.799
IHDI	0.705	0.658	N/A	0.746	0.660	0.710

Data of this table are drawn from the World Bank Western Balkans report 2023 (World Bank. 2023)

2.2 Cyber Security as a practice of defense.

The process of protecting networks, computers, servers, mobile devices, electronic systems, and data against hostile intrusions is known as cyber security. It is often referred to as electronic information security or information technology security. The word may be categorized into a few basic categories and is used in a range of situations, including business and mobile computing.

- Safety of networks.
- Program security.

• Data protection.
• Operative safety.
• Continuity of operations and disaster recovery.
• End-user training.

2.3 The scale of the cyber threat

There is an increasing number of data breaches every year, and the global cyber threat is still evolving at a rapid rate. According to a RiskBased Security analysis, in only the first nine months of 2019, data breaches exposed an astounding 7.9 billion records. The amount of records revealed over the same period in 2018 is less than half (112%) of this statistic.

Most breaches occurred in the medical, retail, and public sectors, and the majority of the instances were caused by malevolent criminals. Because they gather financial and medical data, some of these industries are particularly attractive to cybercriminals; nonetheless, any company that uses a network might become the subject of consumer data breaches, corporate espionage, or customer assaults.

Global investment in cybersecurity solutions is inevitably rising as the danger posed by cyberspace is expected to continue growing in scope. According to Gartner, investment in cybersecurity will top $260 billion worldwide by 2026 and reach $188.3 billion in 2023. In response to the growing cyber danger, governments everywhere have released guidelines meant to assist businesses in putting into place efficient cyber-security procedures.

The National Institute of Standards and Technology (NIST) in the United States has developed a framework for cyber-security. To prevent malicious code from spreading and facilitate early discovery, the architecture suggests ongoing, real-time monitoring of all electronic resources.

2.4 Types of cyber threats

Cybersecurity combats three types of threats:

• Cybercrime includes both individual and group targets who want to disrupt or obtain financial advantage from systems.
• Politically motivated information collection is a common component of cyberattacks.
• The goal of cyberterrorism is to compromise electronic systems to incite fear or panic.

The National Cyber Security Index is a real-time worldwide indicator that assesses how ready a nation is to handle cyber crises and stop cyber attacks. In addition, the NCSI serves as a tool for developing national cyber security competence and a database including publicly accessible evidentiary materials (NCSI, 2023).

The national cyber security framework has guided the development of the NCSI indicators. The primary cyber threats are displayed at the top of the figure:

• Denial of e-services: The inability to access services
• Unauthorized change of data, or a breach of data integrity
• Breach of data confidentiality: secrets are revealed

The regular operation of national information and communication networks, as well as electronic services (especially crucial e-services), are directly impacted by these risks. A nation has to have the necessary resources for incident management, general cyber security development, and baseline cyber security to handle these cyber threats. The NCSI focuses on quantifiable elements of federally implemented cyber security:

• Current laws, including enacted statutes, rules, and decrees.
• Established units, which include departments, organizations, and the like.
• The forms of cooperation: working groups, committees, etc.
• Results: guidelines, drills, tools, websites, applications, etc.

Public evidence serves as the basis for country ratings.

• Legal statutes
• Official records
• Official webpages

2.5 ISO 27001 and cyber security

These days, privacy protection, cybersecurity, and IT security are essential for businesses and organizations. In the current market, businesses want to give their clients trust and show that they are dedicated to protecting the security of the data they handle. To do this, a firm might gain a competitive edge by obtaining certification of an ISO standard or security regulation, which attests to the proper management of security needs in information processing operations. Controls are unquestionably necessary to ensure the security of devices, communication networks, and information assets given the increasing number of security events and assaults on information and IT systems that enterprises are facing. The idea of cybersecurity was born out of this requirement. The goal of these assaults is to get access to access, modify, or destroy sensitive information belonging to organizations.

Adopting strong cybersecurity measures is a difficult task as hackers are always coming up with new ways to launch attacks thanks to the abundance of tools and technology available. Nonetheless, there is a method for putting data and information security measures into place that partly simplifies and normalizes the process of putting these IT security measures into place. These are the information security and cybersecurity-related ISO standards and rules. The International Standards Organization creates and disseminates ISO standards (ISO). These days, these standards are

a vital component of firms' compliance programs, giving them reputation and recognition across borders. Organizations can gain a competitive edge over their rivals by implementing ISO standards because these certified standards are regularly reviewed and audited to ensure compliance, which significantly enhances the organization's reputation with stakeholders like shareholders and clients. ISO standards are categorized into families and given sequential numbers that correspond to the areas they cover. This allows standards related to comparable problems to be grouped. The procedures, rules, guidelines, skill-building, and other aspects of the field they address—security, continuity, quality, etc.—are the focus of these standards and regulations.

The ISO 27000 series of standards is one of them. This group of information security standards lays out the conditions and recommendations for putting in place an Information Security Management System (ISMS) to handle information security inside a company. The primary standard in this group is ISO 27001, which serves as the series benchmark. The criteria for creating, implementing, maintaining, and continuously improving an ISMS are outlined in this standard.

They are safeguarded by the ISO/IEC 27000 set of standards. (2023 ISO). The most well-known international standard for information security management systems (ISMS) and the criteria that need to be met is ISO/IEC 27001. It outlines the conditions that an ISMS ought to fulfill. The ISO/IEC 27001 standard offers guidelines for creating, implementing, maintaining, and continuously improving an information security management system for businesses of all sizes and across all industries. When a corporation or organization complies with ISO/IEC 27001, it indicates that it has implemented a risk management system for the protection of its data and that the system adheres to all of the best practices and guidelines outlined in this international standard.

Managing cyber risks might appear challenging or even unachievable given the surge in cybercrime and the ongoing emergence of new threats. Organizations may become more risk-aware and proactively detect and fix vulnerabilities with the support of ISO/IEC 27001. The information security holistic approach—vetting of people, policy, and technology—is advocated by ISO/IEC 27001. An operational excellence, cyber-resilience, and risk management tool is an information security management system that is put into place by this standard.

An international standard for information security management is ISO/IEC 27001. The purpose of an information security management system (ISMS) is to assist businesses in strengthening the security of the information assets they own. It outlines the requirements for creating, implementing, maintaining, and continuously improving an ISMS. After an audit is completed and the organization satisfies the standard's requirements, it may elect to be certified by an approved certification authority. A comprehensive analysis completed in 2020 (Akinyemi, Schatz, & Rabih. 2020) examined the efficacy of the ISO/IEC 27001 certification procedure and the standard as a whole.

3. Research framework, the purpose of the case study

The context for this research has been Western Balkan nations' ISO 27001 accreditation and cyber security challenges.

1. RQ1: Is there a connection between the ISO 27001 certifications index and the cyber security index?
2. based on this, two theories have been developed:
3. Ho: The ISO 27001 Standard Certifications Index and the Cyber Security Index are unrelated.
4. H1: The ISO 27001 Standard Certifications Index and the Cyber Security Index are related.

... taking into account that there has been little research on the relationships between the ISO 27001 Standard Certifications Index and the Cyber Security Index, as well as the fact that theoretical approaches to these relationships have been developed but that there are no quantitative, statistical, or algebraic arguments about these relationships.

4. Methodology

In particular, prior empirical research has not explained how the Cyber Security Index, ISO 27001 Standard Certifications Index, and quality management influence and connect, despite the importance of these factors being acknowledged in the business and entrepreneurship ecosystem. The few serious theoretical studies that have demonstrated a strong correlation between the Cyber Security Index and ISO 27001 Standard Certifications Index do not use numerical, statistical, or algebraic studies. As a result, a hypothesis that is backed by research and analysis is required. One in-depth case study technique should be used in an exploratory manner to gain a thorough grasp of phenomena and enable a deeper examination of theoretical structures.

The ISO 27001 standard certifications index and the Cyber Security Index (Y) were analyzed using regression. The ISO 27001 Standard Certifications Index was created by the author of this article by dividing the total number of firms in each Western Balkan nation by the number of ISO 27001 Standard Certificates issued. The CSI was derived from the NSCI Report 2022.

1.1 Data collection

• Data for the cyber security index has been gathered from the NCSI Report 2022 (NCSI. 2022), an annual ranking of countries by their capacity for, and success in cyber security.

• Data for ISO 27001 standard certificates has been gathered from the ISO 2022 survey (International Standards Organization. ISO Survey 2022).

• Data for several businesses in Western Balkan countries drawn from national institutes of statistics of Western Balkan countries, and HitHorizon.

1.2 Data analysis

A regressive analysis (inferential statistics) between the Cyber Security Index and ISO 27001 standard certificates Index for 5 Western Balkan Countries (Albania, Bosnia & Herzegovina, Montenegro, North Republic of Macedonia, and Serbia) was performed.

Table 2. *National Cyber Security Index (NCSI Report 2022)*

Rank	Country	National Cyber Security Index
21	Serbia	80.52
54	Albania	62.34
59	North Macedonia	58.44
97	Montenegro	35.06
112	Bosnia and Herzegovina	28.57

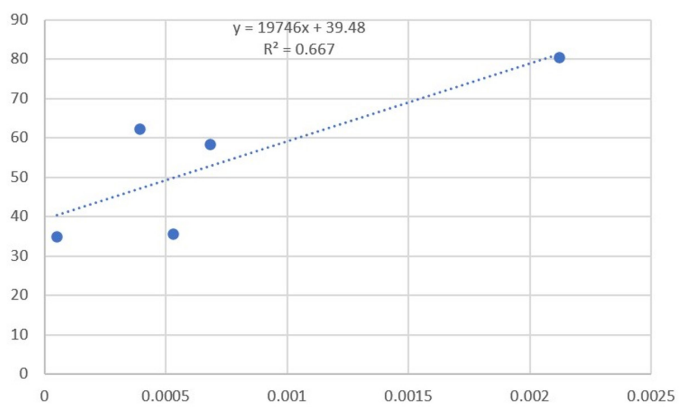
Table 3. *Number of ISO 27001 Standards Certificates, Number of Businesses per WB country, and ISO 27001 Standard Certificates Index.*

No	Country	Number certificates 2022	Variation in number	Variation %	No Businesses	ISO 27001 Standard Certificates Index
1	Albania	49	11	29	125222	0.0003913050
2	Bosnia & Herzegovina	52	5	11	98000	0.0005306122
3	N. R. Macedonia	48	3	7	70424	0.0006815858
4	Montenegro	2	0	0	39682	0.0000504007
5	Serbia	435	8	2	205139	0.0021205134

Table 4. *Regression between Cyber Security Index (Y) and ISO 27001 Standard Certificates Index (X) table*

No	Country	ISO 27001 Standard Certificates Index (X)	Cyber Security Index (Y)
1	Serbia	0.002120513	80.52
2	N. R. Macedonia	0.000681586	58.44
3	Bosnia & Herzegovina	0.000530612	35.57
4	Albania	0.000391305	62.34
5	Montenegro	5.04007E-05	35.06

Graphic 1. *Correlation between ISDO 27001 Standard Certificates Index (X) and Cyber Security Index (Y)*



SUMMARY OUTPUT	
Regression Statistics	
Multiple R	0.816679
R Square	0.666964
Adjusted R Square	0.555952
Standard Error	12.86206
Observations	5

ANOVA					
	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	993.9257	993.9257	6.008045	0.091587
Residual	3	496.2974	165.4325		
Total	4	1490.223			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	39.47992	8.370709	4.716437	0.018049	12.84059	66.11925	12.84059	66.11925
ISO 27001 Index	19746.2	8055.953	2.451131	0.091587	-5891.44	45383.83	-5891.44	45383.83

With these results, we have verified that There is a connection between the Cyber Security Index and the ISO 27001 Standard Certificates Index (Hypothesis 1). R^2 = 0.666964 > 0. 50 (50%).

4.1 Implications for theory and practice

Regarding the theory, a new avenue for investigation into the relationship between the ISO 27001 Standard Certificates Index and the Cyber Security Index has been made possible by the research's conclusive findings. This research views these two indices as instruments for enhancing a business's competitive advantage as well as that of a nation.

4.2 Limitations and further research

Numerous data on the ISO 27001 Standard Certificates for 2022 and the Cyber Security Index have been used in this research, employing a straightforward regression approach to examine the relationship between the two indexes. The statistical analysis results lead to the conclusion of a strong correlation between the two indices, providing a clear and accessible understanding of the relationship, emphasizing the strength of the correlation as a key takeaway from the analysis, however, it is essential to acknowledge a potential limitation regarding the sample size and the temporal horizon of the data. To enhance the future study's validity and applicability, consideration could be given to expanding the sample size by incorporating data from multiple years instead of solely relying on the information from 2022. This would provide a more comprehensive understanding of the trends and relationships over time. To confirm whether these relationships hold for other eras, more investigation is required.

5. Conclusions and recommendations

• A favorable attitude toward cyber security concerns and ISO standards, particularly those about cyber security, particularly ISO 27001, is necessary to achieve a competitive advantage.

• Taking a broader view, this study expands on the general knowledge of cyber security and ISO 27001 standard certification, as well as the relationships between them. It suggests that future research should concentrate on developing and validating the suggested framework and look into the issue in more contexts and settings.
• A regressive study confirmed the strong theoretical relationship between the Cyber Security Index and the ISO 27001 Standard Certification Index for Western Balkan Countries.
• The primary recommendation is that, in response to the path of EU integration, businesses should apply ISO standards more broadly and the ISO 27000 family of standards in particular to become more safe, secure, and guaranteed against cyber-attacks. This will help them remain dependable to their clients and support, improve, and protect business activities, processes, and procedures, giving the Western Balkan economies a competitive advantage.

References

Akinyemi, Iretioluwa; Schatz, Daniel; Bashroush, Rabih (2020). "SWOT analysis of information security management system ISO 27001". International Journal of Services Operations and Informatics. 10 (4): 305. doi:10.1504/ijsoi.2020.111297. ISSN 1741-539X.

Alexander Vezenkov (2017). "Entangled Geographies of the Balkans: The Boundaries of the Region and the Limits of the Discipline". In Roumen Dontchev Daskalov, Tchavdar Marinov (ed.). Entangled Histories of the Balkans – Volume Four: Concepts, Approaches, and (Self-) Representations. Brill. pp. 115–256. ISBN 978-90-04-33782-4.

EU. 2019. SBA Fact Sheet SERBIA. European Commission. https://neighbourhood-enlargement.ec.europa.eu/system/files/2019-11/sba-fs-2019_serbia.pdf

Gray, Colin S.; Sloan, Geoffrey (2014). Geopolitics, Geography and Strategy. Routledge. ISBN 9781135265021.

HitHorizons. 2022. Number of businesses per country. https://www.hithorizons.com/ Retrieved: 16 October 2023.

INSTAT. 2022. Active companies in Albania. https://www.instat.gov.al/en/statistical-literacy/business-register-in-albania/#:~:text=15%2C700%20enterprises%20are%20registered%20during,to%2014%2C946%20registered%20during%202021.

ISO. 2022. ISO survey. https://www.iso.org/the-iso-survey.html

ISO. 2023. ISO 27001 – Information Technology Management. www.osp.org. Retrieved: 16 October 2023.

Kaspersky. 2023. What is Cyber Security? Definition, Types, and User Protection. kaspersky.com. Retrieved on 16 October 2023.

NCSI. 2023. National Cyber Security Index 2022. https://ncsi.ega.ee/ncsi-index/. Retrieved 16 October 2023.

RELEASE 38/2022 2021 Number and structure of business entities in Montenegro. Date of publishing: 30 March 2022. Number of active enterprises, 2021 Final data, 2021 -24.03.2023 Година / Year LXI Број / No: 6.1.23.15State Statistical Office.

Todorova, Maria N. (1997). Imagining the Balkans. New York: Oxford University Press, Inc. p. 27. ISBN 9780195087512.

World Bank. 2023. Western Balkans Spring report. 2023. www.worldbank.org. Retrieved 16 October 2023.