A QUALITY MANAGERIAL APPROACH ON THE RELATIONSHIP BETWEEN THE DIGITAL DEVELOPMENT LEVEL AND THE CYBER SECURITY INDEX

Enriko Ceko [1]

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

Abstract

The main goal for the realization of this study was to verify the level of relations between digitalization and cyber security. The path followed for the realization of this study was the creation of the idea for the study and the relationship between the issues that were considered, the search for the most appropriate and freshest literature, the collection of data for this study, the raising of hypotheses, the processing of data and performing the regression analysis, extracting the results, verifying the main hypothesis, and from them reaching the relevant conclusions and recommendations. The main recommendation of this study is that investment in digitalization also affects investments in cyber security and both together help the development of countries and their integration between each other and beyond, while the relations between digitalization, cyber security and quality management are embodied at ISO standards, especially at ISO 38500, and ISO 27000 family of standards.

Keywords: digitalization, cyber security, regression analysis, ISO standards, quality management.

INTRODUCTION

In order to provide citizens and organizations with quick and simple services, digitalization entails substituting manual procedures with digital ones. In the digital age we live in today, customers are strongly linked to the usage of digital tools, which they use to read newspapers, interact with others, conduct transactions, purchase goods and services, purchase books, make financial decisions, and reserve hotels and holidays. Consequently, digitalization has had a profound impact on the economics of many nations worldwide, especially in certain economic sectors. Technology is evolving and everything will change with it. It is increasingly becoming an indisputable element in raising customer service standards and cutting operating expenses. Innovation is unavoidable and essential. These changes are occurring at an unstoppable rate due to new digital technology. Its revolutionary effect on business and the economy extends far beyond the potential for savings and optimization through the use of information technology advancements (Zërat. 2017). However, security measures must also be used to support digitalization processes, with cyber security being a crucial component.

The protection of computer systems and networks against equipment theft, computer program damage, electronic data theft, and misuse of the services they offer is known as computer security, cyber security, or information technology security (IT security) (Schatz, Daniel; Bashroush, Rabih; Wall, Julie 2017). The growing use of computer systems, the Internet, wireless network standards like Bluetooth and Wi-Fi, and "smart" devices like televisions, smart phones, and other gadgets that make up the "Internet of Things" are all contributing factors to the field's increased importance. One of the biggest issues facing the modern world is cyber security because of its complexity in terms of both politics and technology (Stevens, 2018).

Cybersecurity and digitalization have a significant positive impact on economic and sustainable development in every nation, region, and world at large. Both developed and developing nations invest in cyber security and related digital developments and technologies because failing to do so will cause a gulf between them and hinder communication and international relations, particularly in the areas of business, finance, and economics.

MATERIALS AND METHODS

1. Digitalization

The practice of employing digital tools by individuals, companies, and organizations to increase productivity, value, and speed of work is known as digitalization. For businesses in particular, digitalization is crucial since it may save time and open up new growth prospects.

*Corresponding author:

There are 5.35 billion people using the internet in 2024, equating to 66.2% of the world's total population. Internet users have grown by 1.8% over the past year, with 97 million new users coming online for the first time during 2023 (Kemp. 2024)). This makes the digital world the biggest it has ever been. Businesses are in the forefront of keeping up with the latest advancements in the digital world as we adapt to the technology practices and tools that make up daily life (UT. 2023).

Since technology advancements in the 1990s and 2000s, many organizations have implemented digitalization; yet, its potential applications and advantages are still untapped.

Digitalization is the process of transforming a business's internal operations and opening up new avenues for value and income generation. It entails converting analogue information that already exists into digital formats and a few procedures that businesses can carry out more effectively by utilizing the newest instruments and technologies. Digitalization is a process that involves more than just utilizing computers to record data and going paperless. When fully implemented, digitalization encompasses a network of procedures that leverage digital data to employ technology to expedite activities like accounting, invoicing, and inventory control. Any company that wants to compete in the modern business world must adopt digitalization, especially if they want to cut costs and save time. Whether you're moving from paper to electronic invoicing or completely revamping your sales process for internet optimization, digitization can have a lot of advantages (UT. 2023).

1.1. Digital transformation

More extensive changes are involved in digital transformation than in digitalization. It suggests using digital technology into every aspect of a company's operations. To capitalize on digitization, digital transformation modifies business models, operational procedures, and corporate cultures. Employee remote work enabled by cloud-based solutions is an example of digital transformation.

1.2. How businesses use digitalization

Diverse company models employ various forms of digitalization. While some businesses may wish to go digital in order to improve customer service, others may choose to do so in order to update their inventory management system.

1.3. Digitalization of products and services

If you are a product or service seller, digitization can help you expand your business. For instance, it can facilitate the creation of digital supply chains with real-time data collection at each stage and facilitate the tracking and management of items (UT. 2023). Having data at your fingertips allows you to quickly spot patterns, problems, bottlenecks, and inefficiencies and find solutions. The following are some instances of digitized goods and services:

- Enabling consumers to pay for goods via an app;
- Using a central digital database to store and retrieve patient medical records;
- Adding a barcode or QR code to products.
- Putting your company at the forefront of your product or service online;
- using a point of sale (POS) device linked to a POS system;
- Digitizing internal processes (UT. 2023)

If the organization trades in real goods, there are several ways in which internal business operations can be digitalized. Inventory management may be exceedingly challenging, especially when done manually. Investing in a digital inventory management system facilitates inventory management and helps to streamline procedures. After that, the goods may be packaged for shipping, precise information on products that have been stored can be obtained, and damaged goods can be located. Issuing digital invoices rather than printing paper invoices helps streamline this process. Because digital invoices are paperless, they are easier to examine and process and are better for the environment. In addition, digital invoices are less prone to errors and require no physical storage space.

The ability of invoicing and inventory systems to interact directly, allowing inventory management to be completed without analogue interaction, is one of the many advantages of digitization with digital invoices. The work-in-process inventory counts are subtracted from the invoiced amount.

Lastly, accounting software helps streamline a company's financial reporting. Digitalization allows for the recording of transactions, the making of entries, and the completion of a final analysis with a few laptop touches.

1.4. Digitizing customer interactions

In a recent survey, 88% of participants said that they thought a company's customer experience was just as essential as its goods or services (SR. 2022). This serves as another evidence that firms should do everything within their power to guarantee that their relationships with clients are fulfilling and constructive. This may be accomplished at scale with the aid of digitalization, which optimizes every digital point of contact between a company and its clients. Software for customer relationship management, for instance, can assist in keeping track of each and every customer encounter. By having access to it, interactions can be tailored to offer individualized services. Additionally, CRMs gather and examine customer-related data that can be utilized to create more effective customer service plans (UT. 2023).

1.5. Digitalization of the supply chain

Managing supply chains by hand could be challenging. Because supply networks are so complex, interdependent, and variable, managing them can be difficult. Thankfully, the procedure has become considerably simpler due to recent advancements in supply chain management technologies. There are various ways to incorporate digital technology into the supply chain:

•The utilization of software for inventory management,
• Demand forecasting,
• Last-mile delivery,
• On-demand storage (UT. 2023)

1.6. The benefits of digitalization

When properly implemented, digitization can:

• Save time by minimizing or doing away with labor-intensive manual data input procedures.
• Enhances business preparedness by empowering you to foresee obstacles and devise strategies to overcome them.
• Enhances workflows through process automation and the reduction or elimination of inefficiencies caused by humans.
• Makes data-driven decisions easier by spotting trends and averting possible issues.
• Lowers errors through process automation that eliminates human error.
• Increases productivity by optimizing available resources.
• Lowers operating costs by lowering the number of workers needed for manual tasks.
• Boosts output by enhancing both team and individual worker productivity.
• By applying digital technologies and strategies around customer-facing procedures, enhance customer engagement and service.
• Enhances data analysis by streamlining the gathering and storing of data and by offering insights to direct business decision-making.
• Facilitates automation by fostering a manual intervention culture that is restricted to tiresome or repetitive dialogues.
• Facilitates quick decision-making by verifying new procedures and reviewing and refining current ones.
• Boost income through the development of sophisticated data-driven automation and efficiency-based sales and marketing systems (UT. 2023).

1.7. Disadvantages of digitalization

Among the possible obstacles to corporate digitalization are:

• Technical difficulties brought on by a lack of skilled workers and the requirement for sufficient labour proficiency in implementing new technologies.
• Decision-making that is stifled by risk aversion, ingrained legacy processes, and silencing.
Employee and management resistance to implementing digitally led systems and processes is a symptom of cultural problems.
• Security and privacy issues pertaining to the cost of cyber security infrastructure, the possibility of malevolent cyberattacks, and regulatory data compliance (UT. 2023).

2. Cyber security

Cybersecurity is the discipline of defending programmes, networks, and systems from online threats. These cyberattacks typically target sensitive data access, alteration, or destruction; ransomware extortion of users' funds; or interference with regular corporate operations (Cisco, 2024). Today's increasingly sophisticated attackers and the fact that there are more devices than people make it particularly difficult to implement effective cybersecurity safeguards. Many levels of security are layered over computers, networks, programmes, and data that one wants to keep safe in a good cybersecurity strategy. To effectively defend against cyberattacks, an organization's people, processes, and technology must work in concert with one another.

People: Users need to be aware of and follow fundamental data security guidelines, like selecting secure passwords, being cautious when opening emails, and regularly backing up their data (Cisco, 2024).

Processes: Businesses need to have a plan in place for handling both successful and attempted cyberattacks. A reputable framework can serve as a reference and provide guidance on how to recognize attacks, safeguard systems, recognize and respond to risks, and recover from successful attacks.

Technology: In order to provide businesses and individuals with the computer security capabilities they need to defend themselves against cyberattacks, technology is needed. Endpoint devices, which include PCs, smart gadgets, and routers; networks; and clouds are the three primary entities that need to be secured. Next-generation firewalls, DNS filtering, antivirus software, malware protection, and email security solutions are among the common technologies utilized to safeguard these companies (Cisco. 2024).

2.1. The importance of cyber security

Everyone benefits from cutting edge cyber security solutions in today's connected environment. Individually, a cyber security breach may lead to identity theft, extortion attempts, or the loss of private information such as family photos. Everybody depends on vital infrastructure, including hospitals, power plants, and financial services firms. The smooth operation of our society depends on the security of these and other organizations (Cisco, 2024).

2.2. Some of the types of cyber security threats

The act of sending bogus emails that appear to be from reliable sources is known as phishing. The intention is to steal private information, including credit card numbers and login credentials. As per Cisco (2024), this is the most prevalent kind of cyberattacks:

1. An adversary may employ social engineering as a strategy to coerce you into disclosing private information. They might ask for money or access to private information. Any of the aforementioned dangers can be paired with social engineering to increase your likelihood of downloading malware, clicking on links, and believing unscrupulous sources.
2. Malicious software includes ransomware. By preventing access to files or the computer system until the ransom is paid, it is intended to extort money. Restoring the system or recovering the files is not assured by paying the ransom.
3. Malware is a category of software intended to damage or obtain unauthorized access to a computer (Cisco, 2024).

3. Quality management and Digitalization (ISO 38500:2024)

Most businesses depend on information technology (IT) to run successfully, both as a supporting function and as a component of their ability to transform themselves. In order to satisfy the demands and expectations of the organization's stakeholders, IT can significantly improve results and facilitate the development of new business models. The ISO 38500 standard, specifically designed for digitization, was created by the International Standards Organization (ISO 2024, a). In order for their organizations to fulfil their mission in a way that their stakeholders anticipate, governing bodies need direction on the responsible, innovative, sustainable, and strategic use of IT, data, and digital capabilities. To accomplish excellent governance, the governing body can use three instruments together with related governance and management practices of IT:

1. IT governance principles: Using these guidelines to ensure that IT is used responsibly and strategically can make an organization more flexible and adaptable.
2. IT Governance Model: This model outlines the primary IT governance duties and their relationships across the entire organization, facilitating decision-making and assigning of roles for all facets of IT use.
3. IT Governance Framework: This helps make sure that the important governance actions are taken into account and applied to the way the organization uses IT. It outlines the components that the organization uses to regulate its IT arrangements.

This document's target audience includes: — all organizations, ranging from small to large, irrespective of the degree of their use of IT; — public and private corporations, government agencies, and non-profit organizations (ISO. 2024, a). It also offers direction to people who advise, inform, or support governing entities.

Among them are the following:

- External business or technical specialists, such as legal or accounting specialists,
- Retail or industrial associations,
- Professional bodies;
- Internal and external service providers (including consultants);
- Auditors (ISO. 2024, b).

Although ISO 38500 was created to direct board oversight of IT, it contains a plethora of helpful guidelines for digital leadership and change (Toomey, 2017).

Digital transformation is a long-term, ongoing process that disrupts and changes society, markets, business, and government rapidly. It is made possible by the creative application of new digital technologies. It upends many preconceived notions, alters established power structures, and generates new value propositions and value perceptions. (Toomey, 2017).

Digital leadership is the ability of corporate executives to recognise and seize opportunities for revolutionary business growth and value through the transformational use of IT in a way that is acceptable, efficient, and successful. For most businesses, a successful digital transformation will include large adjustments to people (abilities, culture, responsibilities), processes, technology, and organization (structure, market). Without the full executive team and the Board working together, success will be elusive. When applied to business strategy and the means of delivering it, the Evaluate, Direct, and Monitor focus areas guarantee that the Board is appropriately involved in navigating the business strategy through times of disruption; choosing the best technology to realise corporate strategy; ensuring that the rest of the organization is aware of the path being taken; and ensuring progress towards the goal (Toomey. 2017).

4. Quality management and cyber security (ISO 27001 Family)

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, an organization can 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.

4.1. Cybersecurity and ISO standards

These days, cybersecurity is truly taking off, but why? It is undeniable that controls are necessary to ensure the security of devices, communication networks, and information assets given the rising number of security events and attacks involving information and IT systems that businesses are facing. The idea of cybersecurity is born out of this requirement. These kinds of assaults seek to gain access to, alter, or delete private information that belongs to organizations (Martin, 2022).

Effective cybersecurity measures are difficult to deploy because cybercriminals are constantly coming up with new ways to carry out their assaults because to the vast array of tools and technology they use. 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). The International Electrotechnical Commission (IEC) and ISO are the world's foremost authorities on standardizing. They create worldwide standards to standardize particular procedures in fields like information security through technical committees made up of ISO and IEC member organizations (Martin, 2022).

These standards now form an essential part of businesses' compliance systems, giving them respect and recognition across the globe. Organizations that implement ISO standards benefit from a distinct advantage over their competitors. This is because the certified standards undergo periodic reviews and audits to ensure compliance, thereby enhancing 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 together. These rules and standards seek to define methods, guidelines, policies, skill development, etc. in relation to the domains they cover (security, continuity, and quality, etc.).

4.2. ISO 27000 Family

ISO 27000 is a set of ISO standards. To manage information security within an organization, this set of information security standards (Martin, 2022). It lays out requirements and principles for putting an Information Security Management System (ISMS) in place. ISO 27001 is the primary standard in this set and serves as the series benchmark. Requirements for the creation, execution, upkeep, and ongoing enhancement of an Information Security Management System are outlined in this standard. Based on the Deming Cycle, often known as PDCA (Plan-Do-Check-Act), is the process of continuous improvement. The remaining family standards aid in the implementation of the ISMS by providing guidance. PDCA, often known as the Deming Cycle, is the foundation of the continuous improvement process (Plan-Do-Check-Act). The other standards in the family act as a roadmap and assistance for putting the ISMS into practice. An additional notable standard is ISO 27001/02. This is a best practice guide that outlines the necessary controls and control objectives for information security (Martin, 2022)

ISO 27031 is a member of the same family, however it has a different objective. This non-certifiable standard acts as a roadmap and offers a range of techniques and protocols for determining elements that enhance an organization's ICT readiness to ensure and strengthen business continuity. In other words, the primary goal of this standard is to guarantee service continuity and the ability of the organization to resume operations in the event of a disaster and return to a pre-agreed operational condition.

From the ISO 27000 family, ISO 27701 is comparable to the standard mentioned above. Additionally, it lays out guidelines for handling, safeguarding, and monitoring the privacy of the company's personal data in accordance with laws and rules like the General Data Protection Regulation (GDPR). It contains recommendations for safeguarding the privacy and confidentiality of personal data handled by an organization, based on the rules, controls, and goals of the ISO 27001 security standard. It should be noted that only with ISO 27001 certification can this standard be met (Martin, 2022).

I an article on the relations between cyber security and ISO 27001 author verifies by a regression analysis the strong relations between two characters (Ceko. 2023).

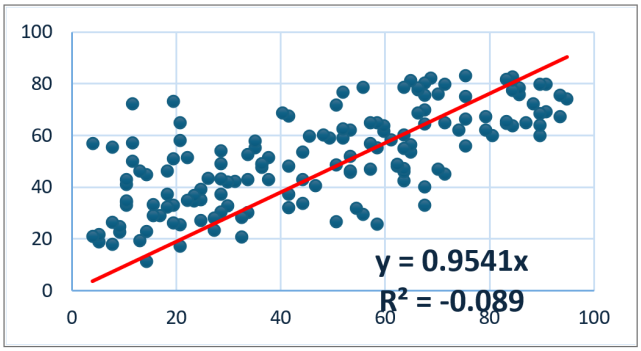
5. Methodology and methods

The process taken to carry out the research project, including coming up with the idea for the study and figuring out how the issues under consideration related to each other, finding the most recent and appropriate literature, gathering data for the study, formulating hypotheses, processing the data and running regression analysis (done by excel), extracting the findings, confirming the main hypothesis, and drawing pertinent conclusions and recommendations from them. The study's principal recommendation is that investments in digitalization have an impact on cyber security investments, and that both positively contribute to national development and intergovernmental integration.

Hypothesis 0: There is no strong relationship between the Level of Digital Development and the Cyber Security Index.

Hypothesis 1: There are strong relationships between the Level of Digital Development (DDL) and the National Cyber Security Index (NCSI).

Graph 1. *Correlation between the Level of digital development and the Cyber Security Index.*



Source: Author of this study.

Tables 1, 2 and 3. *Regression analysis between Level of Digital Development and Cyber Security Index.*

SUMMARY OUTPUT (Table 2)	
Regression Statistics	
Multiple R	0.937599
R Square	0.879092
Adjusted R Square	0.872556
Standard Error	18.69788
Observations	154

ANOVA	(Table 3)				
	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	388916.2	388916.2	1112.426	8.2E-72
Residual	153	53490.45	349.6108		
Total	154	442406.7			

(Table 4)	*Coefficients*	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	0	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A
DDL	0.921394	0.027625	33.35305	4.41E-72	0.866817	0.975971	0.866817	0.975971

Source: Author of this study.

RESULTS

- Through regression analysis, it is proven that there are strong relationships between the Level of Digital Development and the Cyber Security Index, since $R^2 = 0.879092 > 0.50$.
- The results show that Digital Development Level at 87.9092% have the explanation of indication of Cyber Secyrity Index and vice a versa.
- Relations between DDL and CSI are strong (r = 0.937599).
- Regression equation y = 0.9541x
- $R^2 = 0.879092$
- Correlation coefficient "r" = 0.937599.
- Hypothesis H1 – There is a strong relationship between DDL and CSI has been verified.
- By ANOVA Fllog> Fcrit, F Significance F (probability getting these results) < α = 0,05.
- H1 has been verified, with a significance level of 0.05 or a level of reliability = 95 %.
- The H1 has been verified with a significance level 0.1 or a level of reliability = 90% too, and delivers the same result of $R^2 = 0.879092$.
- Coefficients are the values of the correlation coefficient.

CONCLUSIONS AND RECOMMENDATIONS

1. Digitalization is replacing manual processes with digital ones so that citizens and organizations can receive quick and easy services. In the current digital era, consumers are closely associated with the use of digital technologies, which they employ to read newspapers, communicate with others, carry out transactions, buy products and services, buy books, make financial decisions, and book travel and accommodations.
2. As a result (of 1), digitization has significantly impacted the economies of numerous countries throughout the world, particularly in specific economic sectors. Everything is changing in tandem with the evolution of technology. It is undeniably becoming a necessary component for improving customer service standards and reducing operating costs. Innovation is necessary and inevitable. The rapid pace of these changes is attributed to modern digital technology. Beyond the potential for savings and optimization through the application of information technology breakthroughs, it has a revolutionary effect on business and the economy.
3. In every country, every region, and every part of the world, cybersecurity and digitalization have a major positive influence on sustainable and economic development. Investments in

cyber security and related digital innovations and technologies are made by both developed and developing countries since not doing so will widen the gap between them and impede international connections and communication, especially in the fields of commerce, finance, and economics.

4. The process of digitalization involves transforming pre-existing analogue data into digital formats and a few operations that companies can perform more efficiently by employing the newest tools and technologies. It is a process that goes beyond using computers to store information and eliminating printed documents, and when completely executed, entails a web of processes that use digital data to make use of technology in order to accelerate tasks such as inventory control, invoicing, and accounting. Any company that wants to compete in the modern business world must adopt digitalization, especially if they want to cut costs and save time.

5. Real goods trading companies can invest in a digital inventory management system, which makes inventory management easier and streamlines processes. After that, products can be located and packaged for shipping with accurate information on stored goods. This process can also be streamlined by issuing digital invoices instead of paper ones, which are easier to examine and process, better for the environment, less error-prone, and require no physical storage space. While another benefit of digitization with digital invoices is the direct interface between inventory and invoicing systems, which makes it possible to complete inventory management without analogue interaction. The invoiced amount is deducted from the work-in-process inventory counts, while accounting software facilitates the financial reporting of a business, making clear transaction recording, entry, and final analysis can all be completed thanks to digitalization. Customer relationship management software can help maintain a record of every interaction with customers. Access to it allows interactions to be customized to provide personalized offerings, and also collect and analyze client-related data that can be used to develop customer care strategies that are more successful. Handling supply networks by yourself could be difficult. Managing supply networks can be challenging due to their complexity, interdependence, and variability. Thank goodness, new developments in supply chain management systems have made the process much easier. Software for last-mile delivery, demand forecasting, inventory management, on-demand storage, and other related tasks can be used to do this.

6. The innovative use of new digital technologies can enable digital transformation, a protracted, continuous process that quickly upends and modifies markets, industry, government, and society. Numerous preexisting beliefs are turned on their head, existing power structures are changed, and new value propositions and value perceptions are created.

7. The ability of corporate executives to identify and grasp chances for transformative business growth and value through the innovative use of IT in a way that is successful, efficient, and acceptable is known as digital leadership. For the majority of firms, significant changes to people (abilities, culture, responsibilities), processes, technology, and organization (structure, market) are necessary for a successful digital transformation. Success will elude you if the Board and the entire executive staff don't collaborate. The Evaluate, Direct, and Monitor focus areas ensure that the Board is appropriately involved in navigating the business strategy through times of disruption, selecting the best technology to realise corporate strategy, keeping the rest of the organization informed of the path being taken, and ensuring progress towards the goal when it comes to business strategy and the means of delivering it.

8. The majority of organizations rely on information technology (IT) to perform properly, both as a necessary component of their capacity to change and as a supporting role. IT may greatly enhance performance and ease the creation of new business models in order to meet the needs and expectations of the organization's stakeholders. The International Standards Organization developed the ISO 38500 standard especially for digitalization. Governing bodies want guidance on the responsible, innovative, sustainable, and strategic use of IT, data, and digital capabilities so that their organizations may fulfil their mission in a way that their stakeholders anticipate.

9. The discipline of protecting systems, networks, and programmes from internet attacks is known as cybersecurity. These hacks usually aim to interfere with ordinary business operations, extract money from users via ransomware, or access, change, or destroy sensitive data. It is especially challenging to put in place efficient cybersecurity measures because of today's more skilled attackers and the fact that there are more devices than people. A strong cybersecurity plan layers many layers of security over computers, networks, programs, and data that one wishes to keep safe. An organization's people, processes, and technology must cooperate in order to effectively protect against cyberattacks. As a result of these standards, businesses are now respected and recognized globally and are an integral element of their compliance processes. Businesses that use ISO standards have a clear competitive edge over others. This is due to the fact that the organization's reputation with stakeholders, such as shareholders and clients, is improved when the certified standards are subjected to recurring inspections and audits to guarantee compliance. The families of ISO standards are assigned sequential numbers that match the

domains they cover. This makes it possible to group standards pertaining to similar situations together. These regulations and guidelines aim to provide procedures, guidelines, policies, training programs, and other things concerning the areas they address (security, continuity, quality, etc.).

10. Digitalization is the practice of substituting digital procedures for manual ones in order to offer citizens and organizations quick and simple services.

11. Security considerations must be included in digitalization processes, with cyber security being a key consideration.

12. The protection of computer systems and networks against equipment theft, damage, or misuse, as well as against malfunctions or abuse of the services they offer, is known as computer security, cyber security, or information technology security (IT security).

13. Users need to be aware of and follow fundamental data security guidelines, like selecting secure passwords, using caution when opening email attachments, and regularly backing up their data.

14. Businesses ought to have a plan in place for handling both attempted and successful cyberattacks. A reputable framework can serve as a reference and provide guidance on how to recognize attacks, safeguard systems, recognize and respond to risks, and recover from successful attacks.

15. Technology is necessary to provide people and organizations with the computer security tools they need to fend off cyberattacks. Endpoint devices, which include PCs, smart gadgets, and routers; networks; and clouds are the three primary entities that need to be secured. Next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions are examples of common technologies used to safeguard these institutions.

16. Everyone benefits from cutting-edge cyber security solutions in today's linked society. Individually, a cyber security breach may lead to identity theft, extortion attempts, or the loss of private information such as family photos. Critical infrastructure is a necessity for everyone, and the smooth operation of our society depends on the security of these and other institutions.

17. There is a strong relationship between the level of digital development and the cyber security index verified by means of regression analysis where R^2 = 0.879092 > 0.50

18. One of the study's suggestions is that investments in digitalization have an impact on cyber security investments, and that both positively contribute to national development and intergovernmental integration.

Conflict of interests

The author declares no any conflict of interests.

References

1. Carlos Martín. 2022. ISO standards and regulations for improving cybersecurity. https://www.globalsuitesolutions.com/iso-standards-and-regulations-for-improving-cybersecurity/. Visited 20th April 2024.

2. Ceko Enriko. 2023. On relations between Cyber Security Index and ISO 27001 Standard Index in Western Balkan countries. CIT Review Nov issue 2023. https://crj.cit.edu.al/wp-content/uploads/2014/10/crj-nov-issue-2.pdf. Visited 4th May 2024.

3. Cisco. 2024. What Is Cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html. Visited 20th April 2024.

4. International Standards Organization. 2024, a. ISO/IEC 38500 Third edition 2024-02 (en), Information technology — Governance of IT for the organization Technologies de l'information — Gouvernance des technologies de l'information pour l'entreprise, https://cdn.standards.iteh.ai/samples/81684/61bc5f7eee154e2cad5dbdb72f95d208/ISO-IEC-38500-2024.pdf. Visited 20th April 2024.

5. International Standards Organization. 2024, b. ISO/IEC 38500:2024. Information technology. Governance of IT for the organization. https://www.iso.org/standard/81684.html. Visited 20th April 2024.

6. Kemp Simon, 2024. Internet Use in 2024. https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption#:~:text=There%20are%205.35%20billion%20people,the%20first%20time%20during%202023. Visited 4th May 2024.

7. Mark Toomey. 2017. Leading the RoboNDIS campaign. Seeking change and justice for people harmed by bad behaviour in the NDIS. https://www.linkedin.com/pulse/iso-38500-standard-guide-digital-transformation-mark-toomeyISO 38500 - a Standard to Guide Digital Transformation. Visited 20th April 2024.

8. NCSI Report. 2023. https://ncsi.ega.ee/ncsi-index/. Visited 20th April 2024.

9. Salesforce Report. 2022. Nearly 90% Of Buyers Say Experience a Company Provides Matters as Much as Products or Services. https://www.salesforce.com/uk/news/stories/customer-engagement-research/Visited 4th May 2024.

10. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law (në anglisht). 12 (2). ISSN 1558-7215.

11. Stevens, Tim (2018-06-11). "Global Cybersecurity: New Directions in Theory and Methods" (PDF). Politics and Governance. 6 (2): 1–4. doi:10.17645/pag.v6i2.1569.

12. The Upwork Team. Mar 3, 2023. What Is Digitalization in Business? Basics and Best Practices. https://www.upwork.com/resources/digitalization-in-business. Visited 20th April 2024.

13. Zërat. 2017. Ç'farë është digjitalizimi. https://zeri.info/zerat/127535/cfare-eshte-digjitalizimi/. Visited 20th April 2024.

APPENDIXES

Tables 4. *Ranking of countries according to the Level of Digital Development and the Cyber Security Index.*

Rank	Country	NCSI	DDL
1	Belgium	94.81	74.07
2	Lithuania	93.51	67.34
3	Estonia	93.51	75.59
4	Czech Rep	90.91	69.21
5	Germany	90.91	80.01
6	Romania	89.61	59.84
7	Greece	89.61	64.02
8	Portugal	89.61	68.46
9	UK	89.61	79.96
10	Spain	88.31	72.21
11	Poland	87.01	65.03
12	Austria	85.71	75.76
13	Finland	85.71	78.35
14	S. Arabia	84.42	63.89
15	France	84.42	77.29
16	Sweden	84.42	81.51
17	Denmark	84.42	82.68
18	Croatia	83.12	64.63
19	Slovakia	83.12	65.44
20	Netherlands	83.12	81.86
21	Serbia	80.52	59.81
22	Malaysia	79.22	62.19
23	Italy	79.22	67.26
24	Ukraine	75.32	55.96
25	Latvia	75.32	66.23
26	Ireland	75.32	75.18
27	Switzerland	75.32	82.93
28	Bulgaria	74.03	62.06
29	DominicRep	71.43	45.21
30	Russia	71.43	65.12
31	Singapore	71.43	79.93
32	Morocco	70.13	46.88
33	Canada	70.13	75.96
34	Korea Rep	68.83	82.23
35	Bangladesh	67.53	33.11
36	India	67.53	40.02
37	Hungary	67.53	64.25
38	Slovenia	67.53	69.74
39	Israel	67.53	75.50
40	Norway	67.53	80.19
41	Cyprus	66.23	68.83
42	Australia	66.23	77.61
43	Luxembourg	66.23	78.40
44	Georgia	64.94	53.50
45	Thailand	64.94	56.63
46	USA	64.94	81.05
47	Paraguay	63.64	42.58
48	Philippines	63.64	45.99
49	Indonesia	63.64	47.41
50	Azerbaijan	63.64	54.78
51	Argentina	63.64	60.43
52	Japan	63.64	78.69
53	Peru	62.34	48.23
54	Albania	62.34	48.74
55	Türkiye	61.04	58.29
56	Chile	59.74	61.44
57	Uruguay	59.74	63.86
58	Benin	58.44	25.83
59	NRMacedonia	58.44	55.36
60	Qatar	58.44	64.99
61	Egypt	57.14	46.93
62	Moldova	57.14	56.79
63	Bahrain	57.14	65.17
64	Zambia	55.84	29.66
65	Iceland	55.84	78.64
66	Nigeria	54.55	31.76
67	Ecuador	53.25	45.57
68	Tunisia	53.25	46.26
69	Colombia	53.25	52.08
70	Belarus	53.25	62.33
71	Brazil	51.95	59.11
72	China	51.95	62.41
73	New Zealand	51.95	76.81
74	Uganda	50.65	26.71
75	Panama	50.65	48.43
76	Malta	50.65	71.74
77	Costa Rica	49.35	58.87

78	Kazakhstan	48.05	60.18
79	Ghana	46.75	40.68
81	Oman	45.45	59.51
82	Côte d'Ivoire	44.16	33.54
83	Sri Lanka	44.16	43.02
84	Mauritius	44.16	53.57
85	Pakistan	41.56	32.23
86	Kenya	41.56	37.14
87	Jamaica	41.56	48.18
88	Brunei	41.56	67.5
89	UAE	40.26	68.87
91	Kyrgyzstan	37.66	42.96
92	Mexico	37.66	51.46
93	Vietnam	36.36	47.69
94	Uzbekistan	36.36	49.00
95	S. Africa	36.36	49.24
96	Armenia	35.06	55.06
97	Montenegro	35.06	57.79
99	Rwanda	33.77	30.23
100	Algeria	33.77	42.81
101	Trnd&Tbg	33.77	52.6
103	Ethiopia	32.47	20.70
104	Cameroon	32.47	28.28
105	Bolivia	31.17	42.09
107	Nicaragua	29.87	32.70
108	Botswana	29.87	41.96
109	Nepal	28.57	30.58
110	Namibia	28.57	37.28
111	Venezuela	28.57	43.14
112	B&H	28.57	49.31
113	Jordan	28.57	54.07
114	Malawi	27.27	23.20
115	Vanuatu	27.27	28.10
116	Tonga	25.97	43.40
117	Tanzania	24.68	26.96
118	Guatemala	24.68	35.43
119	El Salvador	24.68	39.17
120	Cambodia	23.38	34.59
121	Bhutan	23.38	36.90
122	Honduras	22.08	35.09
123	Suriname	22.08	51.50
126	Chad	20.78	17.28
127	Sudan	20.78	25.50
128	Grenada	20.78	58.00
129	Bahamas	20.78	65.10
131	Mali	19.48	26.00
132	Senegal	19.48	33.04
133	Iran	19.48	51.04
134	Barbados	19.48	73.10
135	Lao PDR	18.18	32.37
136	Belize	18.18	37.10
137	Mongolia	18.18	46.41
139	Cuba	16.88	29.10
140	Zimbabwe	15.58	28.97
141	Syria	15.58	33.40
142	Mauritania	14.29	11.30
143	Madagascar	14.29	22.80
144	Fiji	14.29	44.90
145	Afghanistan	12.99	19.50
146	Saint Lucia	12.99	46.30
147	Seychelles	11.69	50.30
148	Antg&Brbd	11.69	57.10
149	SK&Nevis	11.69	72.40
151	Samoa	10.39	33.00
152	Myanmar	10.39	34.29
153	Tajikistan	10.39	34.56
154	Libya	10.39	41.10
155	Guyana	10.39	42.91
156	Angola	9.09	22.69
157	Mozambique	9.09	24.88
158	Yemen	7.79	18.00
160	Haiti	7.79	26.46
161	SV&Grnd	7.79	55.40
166	Congo	5.19	18.91
167	Kiribati	5.19	21.70
168	Slmn Isl	3.90	21.10
169	Dominica	3.90	56.90

Source: NCSY Report. 2023.