UDC 004.056.5:004.738.5(479.24)
DOI: 10.15587/2706-5448.2025.342927

Khayala Alasgarova,
Sahib Ramazanov

DEVELOPMENT OF STRATEGIES FOR ENHANCING CYBERSECURITY AND DIGITAL TRUST IN AZERBAIJAN'S DIGITAL LANDSCAPE

This research focuses on assessing cybersecurity practices and the level of digital trust in Azerbaijan and identifying key weaknesses using real-world data.

The object of the research is cybersecurity practices and digital trust among organizations and users in Azerbaijan.

The research solves the problem of insufficient empirical data on cybersecurity practices and digital trust in Azerbaijan, which contributes to low awareness, weak security implementation, frequent cyber incidents, and limited trust in digital services and legislation.

The research methodology included a quantitative survey of 129 participants, Spearman correlation analysis, and risk heatmap modeling. Data analysis was conducted using a personal computer with Microsoft Excel and (Statistical Package for the Social Sciences) SPSS software.

The results show that 55% of organizations have moderate cybersecurity awareness, 17.8% have low awareness, and 53.5% do not provide cybersecurity training to employees. Although 76% of banks use multi-factor authentication (MFA), 40.3% have experienced fraud incidents. Spearman correlation analysis indicates a negative relationship between awareness and cyber incidents (–0.33) and between training and incidents (–0.29), while MFA usage shows a positive correlation with fraud detection (+0.3446). In addition, 64.3% of users feel somewhat safe, and 41.1% identify public education as the most important area requiring improvement.

The findings demonstrate that insufficient training, incomplete adoption of modern protective measures, and weak public education increase cybersecurity risks even in organizations with moderate awareness. The results can support the State Service for Special Communication and Information Security (SSSCIS) in improving the National Cybersecurity Strategy and assist banks, businesses, and educational institutions in strengthening cybersecurity practices for the period 2025–2030.

Keywords: *cybersecurity, digital trust, phishing attacks, data breach, fraudulent activities.*

Received: 21.09.2025
Received in revised form: 28.11.2025
Accepted: 23.12.2025
Published: 29.12.2025

How to cite
Alasgarova, K., Ramazanov, S. (2025). Development of strategies for enhancing cybersecurity and digital trust in Azerbaijan's digital landscape. Technology Audit and Production Reserves, 6 (2 (86)), 39–56. https://doi.org/10.15587/2706-5448.2025.342927

1. Introduction

Many countries around the world are going through rapid digital changes that open up new ways for the economy to grow, but they also make cyber threats much more dangerous. According to PricewaterhouseCoopers (PwC) research, the costs of cyber-related events in 2024 were in the billions of dollars around the world, and the average cost of a data breach was higher than ever before. Azerbaijan is also dealing with similar problems as it works to move forward with its digital economy initiative. As online services grow quickly in the banking and public sectors, so do phishing schemes, fake transactions, and ransomware attacks. Without strong cybersecurity rules, digital trust – the confidence that people and businesses have in the safe and ethical use of digital tools – decreases. This makes it harder for people to use electronic services and slows down economic growth.

This document contains a list of definitions that are already in use for cybersecurity and information security. It indicates that the majority of definitions emphasize the protection of confidentiality, integrity, and availability, commonly referred to as the confidentiality, integrity, and availability (CIA triad). However, the challenges regarding the empirical assessment of the actual implementation levels and their effects on digital trust in developing nations remain unaddressed. This is mostly because it costs a lot of money and is hard to organize to do large surveys in these areas, and there aren't any standardized methods that work well in these situations. A potential solution to these challenges is to carry out focused online surveys, followed by statistical correlation evaluations. This method was employed in the research, but it was limited to the analysis of information security, excluding the behavioral aspects of digital trust. This circumstance underscores the imperative for a study centered on the empirical assessment of cybersecurity methodologies and their correlation with the degree of digital trust in Azerbaijan.

The paper [1] provides a compilation of definitions related to cybersecurity and information security from various international organizations and researchers. It points out that there is no one definition that everyone agrees on and that most ideas are based on the triad of confidentiality, integrity, and availability. However, there are still problems with how to use these definitions in practice across the country and how to make them fit the needs of new digital economies. This issue stems from the predominantly theoretical orientation of these collections, which lack empirical substantiation in specific nations.

The paper [2] analyzes the importance of digital trust in reconstructing trust dynamics within the digital society, utilizing trust theory and expectation-confirmation theory. It illustrates that digital trust has a direct impact on how users engage and adopt new technologies. However, this analysis relies solely on theoretical modeling and does not include quantitative insights into how particular cybersecurity

ISSN-L 2664-9969; E-ISSN 2706-5448

practices (such as multi-factor authentication and training frequency) affect trust levels in transitioning economies.

The study [3] explores how digital trust affects the value of firms and their governance by looking at a sample of companies in the United States. It demonstrates that companies with greater digital trust tend to achieve improved financial performance and greater confidence from investors. However, the findings are constrained to the United States (US) market, which has an established regulatory framework, making it difficult to apply the results to nations with emerging legal systems (like Azerbaijan) due to variations in regulations and public understanding.

The article [4] analyzes existing methods and future requirements for cultivating a strong cybersecurity culture within organizations, primarily based on data from the United Kingdom (UK). It suggests that ongoing training in security awareness along with strong commitment from management can significantly lower the prevalence of successful cyber-attacks. Nevertheless, the research does not focus much on the banking sector and overlooks the unique conditions in countries where fast digital growth exceeds the advancement of human skills.

The paper [5] reviews the security of industrial control systems specifically in the context of Azerbaijan. It highlights that essential infrastructure is still susceptible to targeted attacks because of insufficient adoption of contemporary security standards. Nonetheless, this research is limited to the industrial field and does not address the banking sector, public services, or the attitudes of regular users towards digital trust.

All these points suggest the need to undertake a study that thoroughly assesses cybersecurity practices, their actual effectiveness, and their influence on the level of digital trust across various sectors of Azerbaijan's economy. This can be accomplished using a unified questionnaire [3], a diverse sample [4], and statistical correlation analysis – a method that overcomes the geographical and sectoral restrictions found in studies [5] and enriches theoretical frameworks [2] with numerical insights from a specific national environment [1].

The object of research is cybersecurity practices and the degree of digital trust among organizations and users in Azerbaijan.

The aim of this research is to assess the current state of cybersecurity and digital trust in Azerbaijan and to develop practically oriented recommendations for its improvement.

To achieve the aim, the following tasks were solved:

1. To conduct a theoretical analysis of concepts "cybersecurity" and "digital trust" and their interrelation.
2. To develop and conduct a survey of representatives of various sectors of Azerbaijan on the level of awareness, applied measures and experienced incidents.
3. To perform statistical analysis of the obtained data, including correlation and risk mapping.
4. To formulate recommendations for state bodies, banks and organizations to strengthen cybersecurity and increase digital trust.

2. Materials and Methods

2.1. Materials

An extensive review was conducted using academic publications, industry reports, and case studies from sources such as PwC, Gartner, Accenture, KPMG, Statista, and Comparitech. Key references included definitions of cybersecurity [1, 6–9], digital trust analyses [2–4, 10–16], cyber threats in Azerbaijan [5, 17–19], and global comparisons [20–55]. These materials provided foundational theories on the CIA triad (confidentiality, integrity, availability), cyber risks, and digital trust dynamics.

A custom questionnaire titled "Cybersecurity in Azerbaijan" with 12 questions on awareness, practices, incidents, and trust levels. It was distributed anonymously via internal emails and social networks to employees from 30 randomly selected local and international companies in sectors like oil/gas, finance, and government. The survey targeted a sample size of at least 121 (calculated for representativeness) but yielded 129 responses, ensuring confidentiality to encourage honest replies.

Global cybersecurity metrics from Statista (2023) [55] and Comparitech rankings for cross-country analysis.

The materials were received in sequence: literature sources were gathered first (January–March 2025) via online databases and reports; survey data was collected next (April–June 2025) through digital distribution; comparative data was accessed last (July 2025) for integration.

2.2. Cybersecurity

2.2.1. Definition of cybersecurity

The concept of "security" in the modern world plays arguably one of the most crucial roles in all aspects of life: biological, political, economic, social, technical, territorial, and others. Therefore, it is very important not only to correctly define this concept and its derivatives but also to apply them appropriately for their intended purpose. Unfortunately, this highly desirable outcome has not yet been achieved. However, efforts to achieve it continue.

"*Cybersecurity refers to the conditions of protection against physical, spiritual, financial, political, emotional, professional, psychological, educational, or other types of impacts or consequences of accidents, damage, errors, incidents, harm, or any other events in cyberspace that could be deemed undesirable.*" [6] – definition 1.

"*Cybersecurity is a set of conditions under which all components of cyberspace are protected from the maximum possible number of threats and impacts with undesirable consequences.*" [7] – definition 2.

With regard to such definitions, the first thing that must be noted is the use of the generic term, which is improper in both definition 1, where "conditions" is used, and definition 2, where "a set of conditions" is used, as this generic term requires the proper use of "security". It can thus be seen that "cybersecurity" is a term that is based on the generic term "security" such that "cybersecurity" is a subset of "security" that is defined not only with generic terms but also with "specific characteristics" that will comprise the second component of the term "cybersecurity".

Since the generic term used in the selected definitions of "cybersecurity" is not appropriate, it is not reasonable to discuss the second part of these definitions. Further considerations regarding the definition of the term "cybersecurity" are tied to selecting a definition of the term "security" that would allow for the correct formulation of the second part of the definition of "cybersecurity", following the generic term.

In this article, the definition of "security" from definition 3 has been chosen for this purpose:

"*Security is a science that studies natural, technogenic, social, economic, and other processes of formation, development, and interaction of subjects, objects, the environment, and their combinations with the aim of identifying sources of danger, determining their characteristics, and formulating laws and other normative acts that establish concepts, requirements, recommendations, and methodologies, the implementation of which should guarantee the protection of the interests of the individual and society as a whole from all identified and studied sources of danger.*" [8] – definition 3.

Using this method of definition formulation, the following definition of the term "cybersecurity" is proposed:

"*Cybersecurity is a branch of security that studies the processes of formation, functioning, and evolution of cyber objects with the aim of identifying sources of cyber threats that could cause harm to them and formulating laws and other normative acts regulating terms, requirements, rules, recommendations, and methodologies, the implementation of which should guarantee the protection of cyber objects from all known and studied sources of cyber threats.*"

A cyber object here is understood as any object which functioning is carried out with the involvement of programmable means.

It is further noted that the definition of the term "cybersecurity" in definitions 1 and 2 is based on the concept of "cyberspace":

"Cyberspace is a field of activity within the information space. It is formed by connecting the Internet and other telecommunication

networks. Technological infrastructure supports their operation. It includes any human activity-individual, organizational, or governmental-carried out through these networks" as described in definition 2.

In the definition of the term "cyberspace", the generic term "sphere" is also chosen illogically. This term would be appropriate if defining the term "cybersphere". Actually, it would be more accurate to define the concept of "cyberspace" through the concept of a "cyber object" as follows:

"*Cyberspace is the space in which the functioning and interaction of cyber objects take place.*"

In accordance with the recommendations of definition 3, the term "cybersecurity of an object" should be defined as an inherent property of the object to not pose a danger to the surrounding environment during its functioning in all operating modes:

Cybersecurity of an object is a property of the object that characterizes its internal capability to not cause harm to the external environment or to limit the extent of such harm within acceptable norms.

It should be understood that damage to a cyber object is inflicted as a result of deliberately organized cyberattacks. In this article, a cyberattack is understood as a deliberately organized set of actions involving software and technical means (STM) aimed at causing economic, technical, or informational damage. For example, obtaining classified information on various aspects.

Based on the source of organization, cyberattacks can be divided into two groups: external (in relation to the target of the cyberattack) and internal [56].

Cases of external cyberattacks are reported quite frequently, especially on banking networks and financial organizations with the aim of stealing money from the accounts and cards of private users [17]. However, there have also been instances of cyberattacks on nuclear power plants (NPPs). For example, according to [18] "*the head of Iran's Passive Defense Organization, Gholamreza Jalali, stated that Iranian specialists completed an investigation into the circumstances of the cyberattack. According to their findings, the Stuxnet virus, which targeted the Bushehr NPP, was launched from Israel and the U.S. state of Texas. Jalali also suggested that the engineering corporation Siemens, which supplied and installed the Supervisory Control and Data Acquisition (SCADA) data collection and processing system at the NPP, was also involved in the attack. According to the report's authors, the corporation must explain why it provided Iran's "enemies" with SCADA codes, which made the cyberattack possible. At the end of September, Iranian programmers managed to deal with the computer virus, which, according to the head of Iran's Atomic Energy Organization, Ali Akbar, was present on several Personal Computers (PCs) belonging to the NPP staff.*"

According to [19] "*Currently, a group of specialists (or even an individual) is capable of inflicting irreparable harm to the military, economic, technological, political, and informational security of any state using technical and informational means. Therefore, most actions carried out by parties in cyber warfare affect intergovernmental relations and can lead to political confrontation.*"

As the criticized concepts of "Information Security", the following definitions are taken in the article:

"*Information Security is the protection of confidentiality, integrity, and availability of information*" from [9].

"*Information Security is the state of protection of individuals, organizations, and the state and their interests from threats, destructive, and other negative impacts in the information space*" from [1].

The complexity of this concept lies in the fact that the very subject whose security is being defined has not been determined either in terms of its internal structure or its internal properties, which are necessary for formulating security requirements. Even the definition of information itself is currently quite ambiguous and contradictory. Thus, it is not possible to formulate the concept of the security of such a subject based on its internal structure and internal properties.

Moreover, the definition from [1] includes definitions of its components:

– *Confidentiality of information*: A state of information where access to it is granted only to entities with the appropriate rights.

– *Integrity of information*: The prevention of unauthorized modifications to information.

– *Availability of information*: The prevention of hiding information from users with access rights.

It is notable that all these components represent only external actions concerning the information itself: assigning access rights to information; blocking unauthorized modifications to information; and preventing the concealment of information from authorized users.

However, typically, the protection of an object refers to its defense against external sources of danger, while the security of an object refers to its internal property of not being a source of danger to the environment. From this perspective, it is important to distinguish between two terms: "Cyber safety of an object" and "Cyber security of an object". The first term has been defined above, and the second term, in fact, should be defined as follows:

"Cyber security of an object is a property of the object that characterizes its external capabilities to prevent damage from cyberattacks or limit its extent to acceptable norms."

As for the term "information security", it currently makes sense to consider information as a black box, i. e., only in terms of the protection of information. Therefore, the term "security of information" is, at this point in time, defined solely by the intentions of its owner and nothing else.

This provides grounds to assert that the term "information security" is currently fundamentally incorrect (as long as what information is, along with its internal structure and properties, has not been accurately defined). Instead, the term "information protection" can be proposed, using the previously outlined definition by [9]:

"*Information protection is the protection of confidentiality, integrity, and availability of information*", which, in fact, corresponds to the actual state of the issue under consideration.

2.2.2. Key components of cybersecurity

Cyber security refers to protecting computer systems, computer networks, as well as their associated data, from cyber-attacks, hacking, as well as other cyber threats [20]. It consists of technologies, practices, as well as processes that focus on securing computer systems from malicious exploitation.

Key components of cybersecurity are presented in Fig. 1.

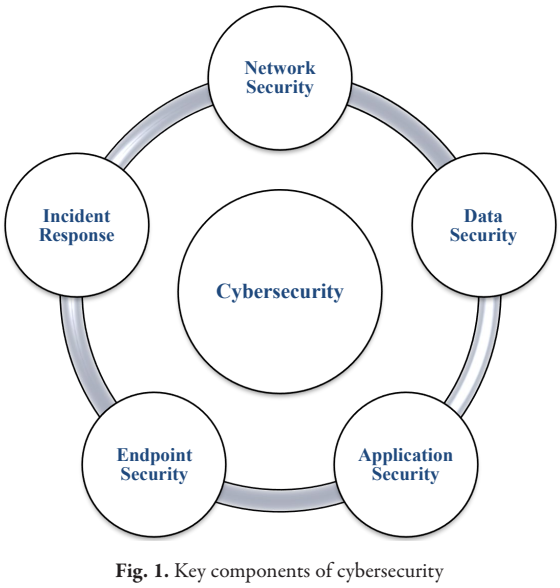

Fig. 1. Key components of cybersecurity

ISSN-L 2664-9969; E-ISSN 2706-5448

As it can be seen, the first key component of cybersecurity is network security.

2.2.3. Network security

At the early stages of network development, security was neither a pressing nor a widely demanded issue, as the Internet was used by a relatively small circle of users. Today, the role of cybersecurity has become increasingly important due to the expansion of computer networks and the Internet into all spheres of life.

The minimum security requirements include installing a firewall at the workstation, which filters incoming data packets. Equally important is the use of the cryptography method for secure data concealment to protect files, and authentication procedures for data access (a common method is entering an authentication code or performing biometric checks) [21]. Modern operating systems are equipped with verification and scanning algorithms that, by filtering various types of information, provide a foundation for data security [22].

In order to secure the data, as well as increase the level of security, the easiest thing that can be done is focusing on strong passwords that can be changed from time to time. Using a password manager, such as LastPass or Sticky Password, is also highly recommended [23]. These applications will be helpful in keeping track of the passwords so that unique strong passwords can be used for accessing different applications as well as different websites, thus providing additional security as the threat of hacking would be reduced. To save the data and improve security, the simplest thing that can be done is set strong passwords and update them periodically [24]. Usually, attackers gain access to the network through old credentials (records), so unused accounts should be deleted [25].

Today, due to the significant influence of the Internet on daily life, cybersecurity has become one of the most critical needs in the world, as cybersecurity threats pose a serious problem for society as a whole and for countries worldwide. Not only should the state disseminate various information among the public, but citizens themselves should also take initiative.

2.2.4. Data or information security

2.2.4.1. Cybersecurity and data security

Cybersecurity is a field of information technology focused on protecting systems that include electronic records, information tracking devices, hardware, and software used to deliver and manage services [26]. Cybersecurity focuses on protecting computer systems against any form of attack through measures that prevent any unauthorized use, as well as the disclosure of data [27]. Essentially, the objective is to guarantee the availability, confidentiality, and integrity of high-value data that, if attacked, may pose human threats.

Cyberspace attacks may be different: some attackers may use ransomware, or they may target individuals' private info. Depending on the scale of the targeted establishment, a cyberattack may also affect them differently. Certain areas that come under this sector with prevalent issues would be: private info, outdated systems, technology issues, as well as security breaks.

Information security (or "InfoSec") is another way of saying "data security", implying the confidentiality, integrity, and availability of data (commonly referred to as the CIA triad) [28]. Most modern business data is stored electronically on servers, desktop computers, laptops, or on the Internet. However, ten years ago, before all sensitive information was moved online, it was stored in archives and offices.

Information security is concerned with ensuring the security of data in any form and is a somewhat broader concept than cybersecurity [29]. Therefore, it can be considered that an information security expert is not necessarily a specialist in cybersecurity.

Cyber security refers to the protection of digital information (e. g. computers, servers, networks, cell phones, etc.) that may be compromised as well as cyber-attacks. It partially encompasses the identification of vital pieces of information, their physical locations, vulnerability, as well as the application of relevant technology to secure them. Information security encompasses physical security [30].

A warehouse full of confidential paper documents requires physical protection. Converting data into digital form necessitates the use of more advanced tools to secure that data. Although it is not feasible to place a lock on a computer, one can be placed on the door of a server room. Regardless of whether the information is stored physically or digitally, a proper physical control measure must be established for its security.

The primary goal of a business focused on information security is to protect a commercial company's data from any form of unauthorized access. The primary goal of a business focused on cybersecurity is to protect the company's data from unauthorized electronic access [31]. However, in both cases, the significance of the data remains paramount.

Both information security and cybersecurity specialists must know which data is most critical for the organization to focus on proper cyber risk management and data control. In some scenarios, an information security specialist may assist a cybersecurity specialist in prioritizing data protection. The cybersecurity specialist would then determine the best course of action for securing the data [32].

However, with the changing security landscape over the past decade, things are not always so straightforward.

During the last ten years, it is possible to see that there is a convergence of cybersecurity experts and information security experts. However, the issue with this convergence is that most of them don't currently employ someone within their firm with information security expertise, causing their responsibilities as cybersecurity experts to greatly increase.

Cybersecurity specialists have traditionally focused on understanding the necessary technologies, firewalls, and intrusion prevention systems, but they have not always been involved in the business aspect of data evaluation [33].

With this topic becoming more relevant within businesses, the involvement of experts in managing cyber risks is transforming in ways that ensure proper data protection. There is greater awareness among business associates as well as investors on the importance of this topic, such that companies must be interested in proper data protection as well as the management of physical and cyber risks.

Cybersecurity is a specific type of information security that focuses on the methods organizations use to protect digital information, such as networks, programs, devices, servers, and other digital assets [34]. Although it is just one aspect of information security (alongside physical security), it receives the most attention because cyber threats are far more likely than physical threats. Malware, criminal hacking, and internal errors are the primary causes of data breaches, so it makes sense to prioritize protection measures that mitigate these risks [35].

Considering the evolution that this field has experienced, there is a clear explanation for why many individuals speak of information security and cybersecurity as if they were the same thing. Indeed, the issues that information security, as well as cybersecurity, aim to address essentially remain the same.

Whether for cybersecurity or information security in general, knowledge of the three pillars of data security is necessary. This framework provides ways, through which security of sensitive information can be achieved, along with:

1. *People*: Employees handle sensitive information daily, so it is crucial for organizations to educate them about risks and how to stay secure.
2. *Processes*: Organizations should document the steps employees must take to maintain security. This includes defining roles and responsibilities for data protection actions.
3. *Technologies*: There is an abundance of technical tools available for organizations to combat threats, such as antivirus software, access controls, and data encryption.

Although there are still lively discussions on the Internet about whether cybersecurity and information security mean the same thing, it makes sense to view cybersecurity as a form of information security. Information security can be seen as an umbrella under which cybersecurity and other security topics, such as cryptography and mobile computing, fall [36]. However, drawing a clear distinction can be challenging, given their mutual placement within a descriptive hierarchy and their overlapping influence.

There are additional differences in the discussion of cybersecurity and information security. While cybersecurity is concerned with protecting information in cyberspace, information security encompasses the protection of data both within and outside cyberspace [37]. In other words, the Internet or an endpoint device may only represent part of the broader picture.

Both cover the protection of cyberspace against any breach that might involve ransomware, spyware, malware, and other forms of malicious software that might cause different types of disruptions. However, experts in cybersecurity may focus more narrowly.

Cybersecurity experts are also taking a proactive approach in securing servers, endpoints, databases, as well as networks, through vulnerability identification and configuration errors that can pose weaknesses [38]. This is right, as they mean that experts prevent a breach. However, the best individuals always think like hackers, or even better, some may come from this background.

Of course, information security experts also focus on protecting against the risk of lost data. They address this concern together with other cyber security experts, although their responsibilities might also involve focusing on the most private information that would likely be targeted in such occurrences.

Table 1 provides comparative characteristics of specialists in these two fields.

Table 1

Comparative characteristics of IT specialists

Computer security IT	Information security IT
Focuses exclusively on online threats	Views the security landscape from afar
Learn to think like a hacker	Engaged in protecting data from any threats
Develops deep understanding of malware	Monitors for unauthorized access/modification/violation
Acts as a first line of defense	Creates plans to recover from a breach

It is also helpful to consider the difference between data and information on a more fundamental level. Data can be anything, such as a series of numbers, but not all data is equal. Determining what this data represents and how confidential it is falls under the purview of information security professionals.

For example, if a series of numbers is a customer's credit card number, information security teams are responsible for ensuring compliance with government regulations. Again, they work closely with their cybersecurity colleagues to secure the most critical data. However, they are responsible for a significantly larger share of the organization's overall security.

Table 2 presents the distinguishing features between information security and cybersecurity.

The Center for Cyber and Information Security defines information security as the process of protecting information and information systems from unauthorized access, disclosure, disruption, destruction, modification, or use, all to ensure confidentiality, integrity, and availability [1]. These three terms are defined as follows:

1. *Confidentiality* – refers to maintaining authorized restrictions on access and disclosure, including measures to protect personal and confidential information [39].
2. *Integrity* – refers to protection against unauthorized destruction or modification of information, including ensuring its authenticity and non-repudiation.
3. *Availability* – refers to ensuring reliable and timely access to and use of information.

Five key differences between the concepts of "cybersecurity" and "information security" are provided below [40]:

Definition – cybersecurity is the practice of protecting data, related technologies, and storage sources from threats. On the other hand, information security means protecting information from unauthorized access that can lead to undesirable changes or deletion of data. Essentially, cybersecurity is the cyber sphere and the data associated with it. Information security, on the contrary, is primarily focused on information, ensuring confidentiality, integrity, and availability.

Domain – cybersecurity means protecting everything present in cyberspace, such as data, information, devices, and technologies related to the above. Information security, on the other hand, concerns the protection of both forms of information – digital and analog – regardless of the domain. Protecting profiles on social networks and personal information in cyberspace is related to cybersecurity. Information security, on the contrary, deals specifically with information assets, availability, and confidentiality of integrity.

Process – while cybersecurity is primarily related to protecting the use of cyberspace and preventing cyberattacks, information security simply protects information from any form of threat and prevents such threatening scenarios.

Professionals – professionals dealing with information security form the foundation of data security and prioritize resources before combating threats. Cybersecurity specialists deal precisely with constant threats of increased complexity.

Protection – cybersecurity eliminates all dangers lurking in cyberspace. Information security, on the contrary, deals only with all forms of threats to information.

Table 2

Differences between information security and cybersecurity

Feature	Cybersecurity	Information security
Definition	The practice of protecting data from external threats in Internet resources	Protects information from unauthorized access, modification, or deletion to ensure confidentiality
Primary focus	Protecting cyberspace from cyberattacks	Protecting information from any form of threats
Scope of protection	Focused on securing the entire perimeter in cyberspace	Ensures protection of information regardless of its domain
Threats addressed	Eliminates dangers to cyberspace	Addresses threats to data in any form
Key objective	Prevents cybercrimes, cyber fraud, and supports law enforcement agencies	Combats unauthorized access, breaches of integrity, and disclosure of information
Collaboration	Assists specialists under constant threat of data breaches	Prioritizes resources to address information threats
Domain of concern	Deals with problems and threats arising in cyberspace	Concerned with information assets, ensuring their integrity and confidentiality

ISSN-L 2664-9969; E-ISSN 2706-5448

Cybersecurity specifically concerns cybercrimes, cyber fraud, and law enforcement agencies. Changing and violating information disclosure, as well as unauthorized access, are two of the most important problems faced by information security.

2.2.4.2. Synergy of cybersecurity and information security

Earlier, the theoretical differences between cybersecurity and information security were primarily highlighted. From a practical perspective, cybersecurity and information security are often treated as synonyms due to their partially overlapping nature in terms of processes, focus, and objectives.

The only way to protect one from malicious actors attempting to use attacks for destruction is to stay ahead of the game and anticipate their next move. This is precisely the aim of advanced research in cybersecurity and information security [39]. As the frequency, intensity, and scale of attacks and cyberattacks continue to grow, this has become more critical than ever before.

Both cybersecurity and information security must work in synergy within the modern interconnected digital ecosystem. Although both technologies address the same objective, that being the safeguarding of valuable information, they do so with different focuses. Collectively, they offer a well-rounded approach being applied towards securing digital assets in the increasingly complex threat environment [41].

Points of convergence for cyber security and information security show that both subjects relate to each other. Both cyber security and information security thus share a basic objective, which involves protecting critical information from any sort of unauthorized access, modification, or deletion. They also depend on each other, as the efficiency of information security is dependent on strong cyber security for protecting digital assets, while cyber security plans depend on information security principles that focus on protecting valuable information. Both also use physical security practices that prevent unauthorized use of vital information [42].

There is synergy between the application of cybersecurity and information security. In risk management, information security experts usually focus on the classification of sensitive information, whereas the application of cybersecurity is centered on finding solutions for digital risks [43]. In incident response, experts in cybersecurity respond to events such as cyber-attacks, malware, and other real-time events, whereas information security focuses on compliance with regulations with respect to restoring businesses [44]. There is also a synergy between the two in terms of staffing, as both deal with educating people on issues such as human error, which remains a threat despite technological advancements.

There are several important advantages of the convergence of cybersecurity and information security. By offering broad-based security, the safety of the information across physical as well as digital platforms gets ensured. By leveraging knowledge from both areas, better threat detection capabilities can be achieved, allowing faster detection of vulnerabilities as well as threats that might emerge. Also, this convergent knowledge helps in compliance with regulatory laws that often cover both digital as well as physical aspects.

Thus, it can be said that cybersecurity encompasses all aspects of security related to cyberspace, whereas information security pertains to the security of information regardless of its field of application. It can be concluded that information security is a superset of cybersecurity. Therefore, endless debates about cybersecurity and information security may be the wrong approach to two concepts that so complement each other and protect data from theft, access, alteration, or deletion. In our view, the main difference lies in the breadth of their focus.

2.2.4.3. Application of artificial intelligence in ensuring data security

Information security, given the increasing adoption and use of computer systems, plays a mandatory role in the modern world. Everyone, whether an individual or a company, seeks to reduce the risk of theft, deletion, or modification of their information. Cybersecurity also plays a significant role in automated systems.

Top companies today integrate dozens of different security products, but they still worry about being susceptible to attack. However, this illustrates that despite greater investment in security, the number of security breaks shows neither signs of slowing down nor stopping.

The implementation of advanced cybersecurity technologies requires time, enabling detailed attack detection and faster resolution than traditional cybersecurity specialists. Artificial intelligence (AI) can serve as one such technology [45]. AI is a technology capable of detecting threats and automatically taking necessary actions to eliminate and prevent them, among other functionalities (Fig. 2).

The figures in the graph correspond to an arbitrary scale of the level of perceived impact from artificial intelligence (AI) in different spheres. These figures offer a relative measure of the extent of contributions that AI may have in terms of advancements or solutions in those spheres.

For example, the importance of cybersecurity is rated the highest, showing that the applications of AI in this field are of great importance as it deals with securing systems, threat detection, and protection from cyberattacks, as well as automated response protocols for securing valuable information.

The healthcare industry is closely tracking this, given the paradigm shift that AI technologies have caused in terms of diagnosis, tailoring treatments, as well as different areas of healthcare research. It is of a higher value, implying its importance in terms of enhanced patient care as well as the healthcare industry.

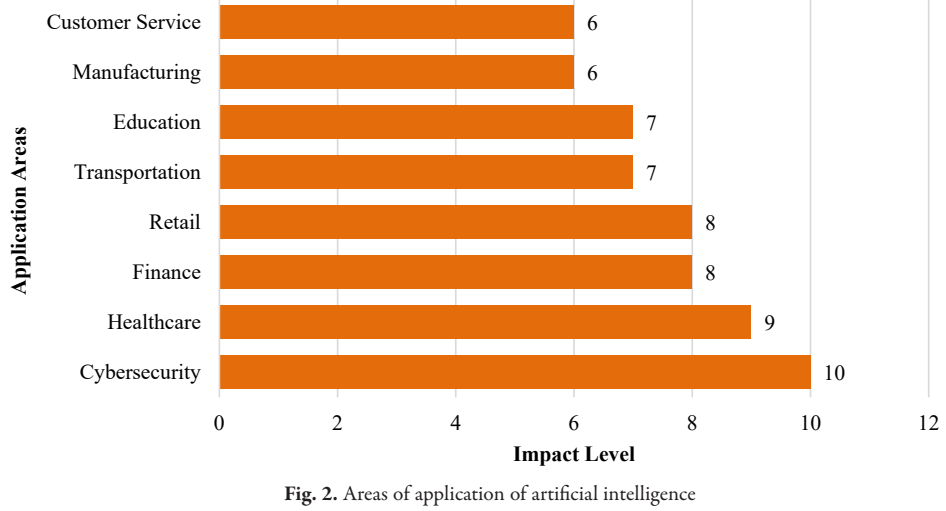

Fig. 2. Areas of application of artificial intelligence

Finance shows a slightly low value, implying that although fraud detection, trading, and risk management systems use AI extensively, its importance is still slightly less than that in the cybersecurity or healthcare industries. Retail, with the same value, deals with the use of AI that helps enhance the customer experience, as well as simplify day-to-day tasks such as inventory control.

Transportation, with moderate value, shows that AI plays a crucial role in the development of self-driving cars, traffic optimization, and infrastructure. Education and manufacturing come next, with slightly low value, showing that AI applications, though vital, are less important compared to other industries. In education, personalized education, and in manufacturing, efficiency.

Customer service has the lowest impact score in this scale, recognizing that although the use of AI technology such as chatbots or virtual assistants is strategic, its application is relatively more restricted in terms of scope compared with others.

AI-based tools address various needs in cybersecurity as follows [46]:

Biometric authentication – passwords can be hacked, compromising critical information belonging to users, businesses, or government agencies. This is where AI-based authentication, such as fingerprint and palm scanning, offers significantly greater security. The system can reliably scan biometric data. When biometric logins are combined with passwords, the likelihood of user data being compromised is greatly reduced.

Accelerating threat detection – traditional cybersecurity systems are not capable of simultaneously handling various types of malware. Also, with improvements in the standards of cyber security, hackers have become more sophisticated. AI helps in recognizing threats as well as responding to them faster, keeping up with the increasing cyber threats. In order to effectively detect advanced persistent threat (APT), the most recent-security tools that can respond to such threats must be used. Companies are implementing AI-driven systems that can easily detect threats through pattern recognition using advanced algorithms and continuously updated codes. AI, combined with machine learning, is highly effective in analyzing website navigation paths, micro-behaviors of malware, and any malicious actions. This analysis further assists in making informed decisions to counter threats effectively.

Rapid response to attacks – simply detecting threats in real time is meaningless if the system cannot combat and prevent them before they cause even minor damage to the system. When a team of hackers attacks a system from multiple points, AI immediately connects the dots and automatically proposes plans to prevent the attack. AI uses intelligent analytics, offering a faster and simpler approach to identifying and neutralizing attacks. For instance, when an AI system detects a malicious file, it prioritizes isolating the file from the system.

Creating a dynamic authentication environment – data can also is intercepted within networks, creating a worrisome situation for employees accessing systems remotely. This means traditional authentication models are no longer secure. Here, AI comes to the rescue. AI systems establish a global, real-time authentication environment that adjusts access privileges based on location or network, utilizing multi-factor authentication. This includes collecting data and analyzing user behavior within the application, device, and network during remote access to data.

Reducing human involvement – no machine can surpass the creativity, imagination, and critical thinking abilities of humans. However, decisions made by engineers are bolstered by the correct data set, informed opinions, and current trends. AI systems significantly reduce human involvement in repetitive tasks while enabling humans to focus on higher-order strategic decision-making. Studying and utilizing meaningful data is time-consuming, making it impossible to address high-risk tasks instantly. When companies develop a secure application using AI technology, security personnel benefit from a respite as threat detection and prevention are automated without human intervention. Continuous user behavior analysis, combined with predictive analytics, reduces the need for engineers to intervene in protecting systems from a series of attacks. The time saved can be reinvested into creative and productive endeavors.

In Fig. 3, AI investment by industry in 2023 is presented.

Based on data from Statista, in 2023, the banking sector led global investments in artificial intelligence (AI), allocating approximately 20.6 billion USD, which constituted 13.4% of the total AI-centric system expenditures. The retail industry followed closely, investing around 19.7 billion USD, representing 12.8% of the global AI spending.

Nevertheless, AI systems are trained and managed by humans, and in some cases, the involvement of human engineers is essential. Humans are capable of going beyond the anomalies that machines may fail to detect and can verify whether a suspected attack is genuine.

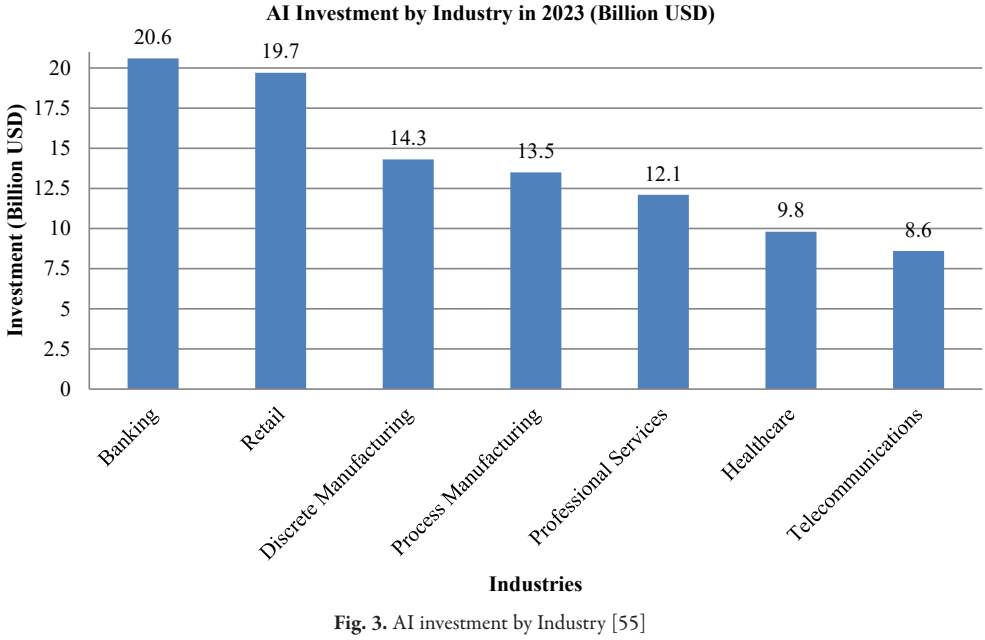

Fig. 3. AI investment by Industry [55]

ISSN-L 2664-9969; E-ISSN 2706-5448

2.2.5. Cybersecurity: problems and solutions

Topics related to cybersecurity are increasingly being discussed across various companies at all levels of management.

A survey of executives in the United States revealed that 50% of them are "highly concerned" about cyber threats [47]. In today's environment, this topic is one of the most frequently addressed during board meetings. At the same time, a significant number of investors view cyberattacks as a substantial risk to their portfolios. Cybersecurity is gaining popularity both abroad and in the United States as a critical area of focus.

The primary goal of cybersecurity is to simplify programs that manage cyber risks, making it feasible for any company to implement them. These programs are tailored to the specific conditions of the company, its needs, risk appetite, and existing threats. When developing an annual plan, the internal audit department should focus on risk assessment, taking into account the perspectives of the board of directors and management [48].

Cybersecurity can be achieved through actions such as asset inventory, analysis and risk evaluation, threat identification, security and change management, ensuring business continuity, and rapid response to external changes, among others.

The fundamental principles of cybersecurity, the violation of which can lead to negative consequences can be considered as follows [49]:

1. *Violation of Integrity*: unauthorized modifications to company data, such as altering the payment details of a counterparty to redirect payments, can result in financial losses and operational disruptions.

2. *Violation of Confidentiality*: breaches of confidentiality can lead to customer attrition or loss of competitive advantage, damaging the company's reputation and market position.

3. *Violation of Availability*: lack of availability of the information system may bring the entire organizational processes to a standstill, thereby resorting to paperwork as a stopgap arrangement. This will not only cause delays but also necessitate re-entry of the information into the system once it's up and running.

In some cases, production-related attacks can cause months-long shutdowns, allowing competitors to secure lucrative contracts. Examples of such disruptions include:

– *Power outages* at aluminum plants, leading to aluminum solidifying in electrolysis baths and resulting in multimillion-dollar expenses for equipment replacement.

– *Disabling of gas turbines*, this can halt operations and incur substantial financial and operational losses.

These scenarios emphasize the critical importance of maintaining the integrity, confidentiality, and availability of systems to protect businesses from severe consequences.

Cybersecurity is ensured through the following stages of [50]:

1. Audit, Examination, or Compliance Assessment. This involves evaluating compliance with internal or external standards and regulatory documents. An audit compares the current state with the required state, while an examination analyzes the current and target states. These steps are essential for the initial collection of information about automated process control systems (APCS) in use, the infrastructure of the protected objects, and the operational technical and organizational security measures.

Procedures during an audit or examination include:

– analyzing operational and design documentation;

– conducting interviews with employees;

– reviewing existing policies, conditions, and organizational and technical measures for data protection;

– examining the network architecture, capabilities, functions, and configurations of APCS software and hardware.

After getting the right data, the next steps are as follows:

– look at automated technology and workflows;

– find the most important nodes and information paths;

– find and evaluate important assets and weaknesses.

After getting the right information, the next steps are:

– look into automated technology and workflows;

– find important nodes and paths of information;

– find and evaluate important assets and weaknesses;

– predict possible threats;

– figure out the current security situation;

– make requirements and suggestions for putting cybersecurity plans into action.

This thorough approach gives a deep understanding of the current security situation and points out areas that need work to make the whole cybersecurity framework stronger.

2. Making a system for cybersecurity measures. After risks are looked at and a threat model is made, a full set of organizational and technical cybersecurity measures is put together. These steps are meant to:

– limit the software environment;

– keep viruses out;

– stop malicious attacks;

– keep an eye on and analyze information security;

– figure out threats and risks that could come from possible attacks.

Adding cybersecurity measures to organizational processes helps with the following tasks – ongoing research and assessment of risks, such as regular updates to the threat and attacker model.

Adding cybersecurity measures to your organization's processes helps with the following:

– ongoing research and assessment of risks, including regular updates to the threat and attacker model;

– overseeing access controls, antivirus protection, cybersecurity incident audits, and security;

– creating and coordinating an emergency action plan: This step makes sure that cybersecurity is backed up by a well-organized and flexible plan that lets businesses deal with new threats while keeping important systems and data safe.

3. Setting up cybersecurity systems for APCs. Before the cybersecurity system goes live, tests are done to see if the protective tools and automated process control systems (APCs) work together. Before the cybersecurity system goes live, tests are done to make sure those protective tools and automated process control systems (APCs) work together. During the testing phase, the performance of the installed technical and software tools and the consistency of the technical processes are evaluated. During the testing phase, ongoing monitoring is done to keep an eye on how well the installed technical and software tools are working and how well the technical processes are working. This makes sure that everything works together smoothly and checks that the system can protect important operations.

4. Keeping APCs' cybersecurity systems up to date. This phase involves performing various support tasks, including:

– providing consulting services related to the installation, operation, and updates of security tools;

– conducting follow-up audits and risk assessments to verify the ongoing effectiveness of cybersecurity measures. This phase emphasizes the importance of continuous support and evaluation to adapt to new threats and maintain a high level of system security [5].

According to the audit results, it is preferable to create two reports. One should be intended for IT specialists and include a detailed description of deficiencies using specific IT terminology. The other should be for top management and the audit committee, containing a description of key factors in "business language".

The British company Comparitech compiled a ranking of 60 countries based on their level of cybersecurity, evaluating the following indicators: the percentage of computers and mobile phones infected with viruses, countries' readiness for hacker attacks, and timely updates to legislation in this field. Among the countries where legislation adapts promptly to changes in cybersecurity were Russia, France, Germany, and China [51]. Fig. 4 illustrates cybersecurity levels by country.

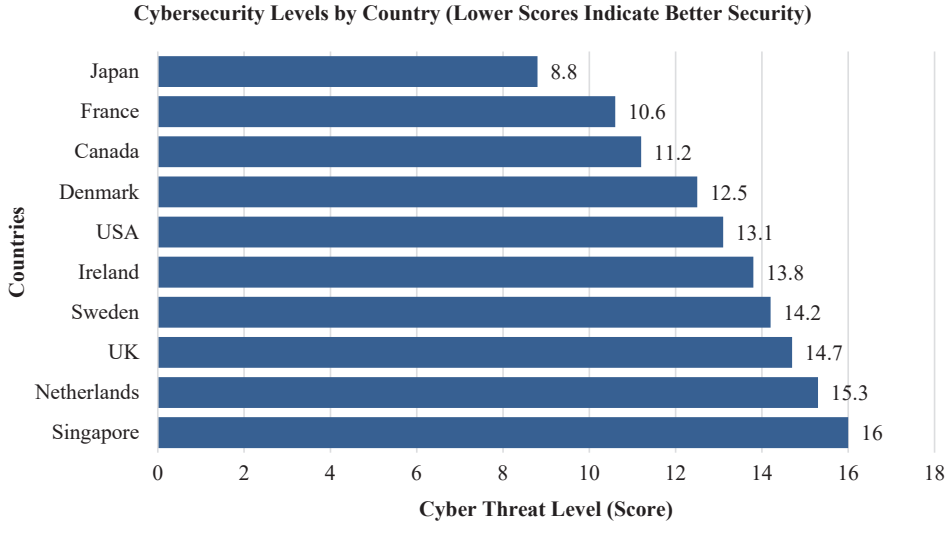

Fig. 4. Cybersecurity levels by country [55]

Fig. 4 presents a selection of 10 countries out of the 60 evaluated in the cybersecurity ranking. Japan is the leader, with a score of just 8.8 in terms of cyber threats (lower scores indicate a better cybersecurity situation). France and Canada occupy the second and third positions with scores of 10.6 and 11.2, respectively. The top 10 also include Denmark, the USA, Ireland, Sweden, the United Kingdom, the Netherlands, and Singapore. The worst-performing countries in this ranking are Algeria (55.75), Indonesia (54.9), and Vietnam (52.44).

The percentage of phones infected with malware is highest in Bangladesh, with 35.9% of all devices used by the country's population affected. In comparison, this figure is 1.34% in Japan. The highest number of infected PCs was found in Algeria – 32.4% (8.3% in Japan). Germany experienced the highest number of attacks aimed at stealing money, affecting 3% of users compared to 0.5% in Japan. Singapore is the most prepared for cyberattacks, while Vietnam is the least prepared. In developing countries, industrial devices are predominantly affected by cyber threats. The countries most heavily targeted by attacks include Vietnam (75.1%), Algeria (71.6%), and Morocco (64.8%). Conversely, the safest countries in this category of cybersecurity are Denmark (14%), Ireland (14.4%), and Switzerland (15.9%) (Fig. 5). The total global damage from cybercrime is estimated to range from 500 billion USD to 1 trillion USD per year [52].

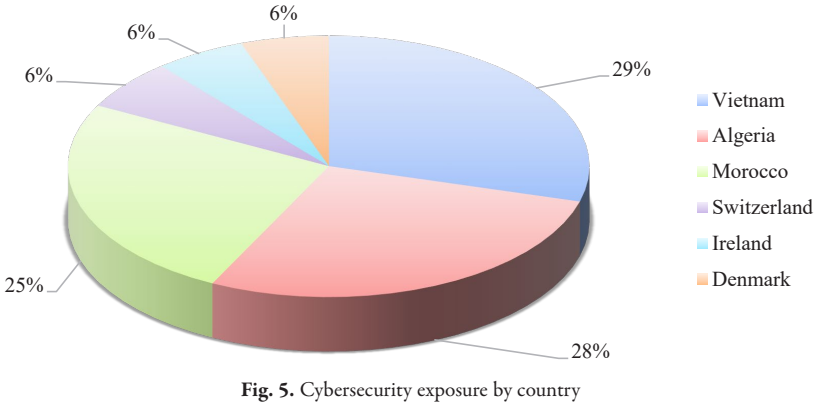

Fig. 5. Cybersecurity exposure by country

Criminals are increasingly targeting mobile phone, smartphone, and tablet owners to spread banking trojans, with the aim of stealing either financial assets or sensitive banking card information.

In order to ensure that there is a low threat of cyberattacks, testing, resource inventory, as well as the analysis of security incidents, must be undertaken. This must be carried out alongside analysis of system events, as well as the perpetual protection of servers as well as web applications. Also, experts in the field of cybersecurity must be involved.

2.3. Digital trust

Currently, the world is in the stage of the digital economy, with its development becoming a strategic task for most nations. The digital economy is built based on such fundamentally new technologies as artificial intelligence, big data, the IoT, quantum and post-quantum cryptography, silicon photonics, distributed ledger technology, and others [53].

Digitalization is increasingly becoming a key driving force behind global inclusive economic growth, transforming industries and creating new opportunities for innovation and efficiency on a worldwide scale [2].

Trust plays a mandatory role in the development of the digital economy. As the digital world increasingly permeates various aspects of our lives, analysing the degree of trust people place in digital devices, services, and the organizations behind them becomes ever more important.

In the G20 Ministers' Statement on Trade and Digital Economy (Japan, June 8–9, 2019), it was explicitly stated that countries must promote trust in the digital economy to harness the benefits of digitalization and address the challenges it brings. The statement emphasized that the digital society should be built on trust among all stakeholders, including governments, civil society, international organizations, academia, and businesses [54]. This trust is fostered through the sharing of common values and principles such as equality, fairness, transparency, and accountability, all while considering the development of the global economy and ensuring functional interoperability.

Currently, many aspects of digitalization remain insufficiently explored. This includes issues such as the adaptation of the labor market to changes in business processes, the development of training systems for the digital economy, and the regulation of new technology implementation.

Among these challenges are questions of digital trust – trust in digital technologies, platforms, and digital institutions. According to data from the renowned research and consulting firm Gartner, trust in social networks and other digital institutions has declined, while concerns regarding data protection and privacy continue to grow.

ISSN-L 2664-9969; E-ISSN 2706-5448

2.3.1. Essence and measures of increasing digital trust

The concept of "digital trust" has relatively recently entered the realm of academic research. Alongside this term, other related concepts are also used, such as "unified electronic trust space" and "digital trust environment". As part of regulatory measures, it is proposed to create legal conditions for the formation of a unified digital trust environment that will provide participants in the digital economy with means for trusted digital remote communications. However, a theoretical analysis of digital trust is practically absent, indicating a gap in comprehensive academic exploration and a need for further research in this area [10].

In English-language literature, the terms "digital trust" and "the digital trust environment" are commonly used. Among international studies on digital trust, notable examples include research conducted by Klynveld Peat Marwick Goerdeler (KPMG), one of the world's largest auditing firms [11], and Accenture, a global professional services and digital technology company [12].

It is important to note that many studies on digital trust are practically oriented, offering diverse interpretations of what digital trust entails. Therefore, the goal of our research is to synthesize existing material on this topic and conduct a comparative analysis of various perspectives on the nature and forms (or directions) of digital trust.

In a study by Accenture, digital trust is viewed not as a technology or process, but as secure, transparent relationships and interactions between a company, its employees, partners, and customers [13]. According to [14], digital trust includes elements such as convenience, user experience, reputation, transparency, and integrity.

The most in-depth research on digital trust was conducted by [3, 15]. They arrived at two key conclusions:

a) trust is a critical factor that determines a country's competitiveness in the digital economy;

b) to sustain the pace of innovative development, providers and government authorities must prioritize increasing the level of trust in digital technologies.

Digital trust level is measured on the basis of the extent of confidence that the users, as well as employees, exhibit in the firm's capability for protecting their personal information as well as the privacy of users of digital services. Digital trust variables comprise elements such as security, confidentiality, reliability, as well as integrity within the authenticity context of digital services.

How can trust in digital technologies be increased among citizens and businesses?

According to Tim Clough, a partner and leader in the Risk Assurance and Corporate Governance practice at PwC, trust in digital technologies, combined with a new approach to risk management, will allow organizations to fully realize their potential. He identified seven areas in the field of digital technologies that can already provide a boost for business development, all of which are grounded in trust [16]. These areas are:

- social networks;
- mobile technologies;
- data analytics;
- cloud technologies;
- digital identity management;
- pace of technological change.

These trust-based digital technologies are essential drivers for the growth and transformation of modern businesses.

Therefore, the enhancement of digital trust emerges as the necessary prerequisite for the adoption of digital technologies, as well as one of the most essential tools for developing businesses. Digital trust-building is a process that takes time, necessitating joint activity on the part of all participants, such as governments, companies, as well as individuals.

However, further scientific studies on this topic are necessary, taking into consideration its novelty as well as the fast-paced development of digital technology. Thorough investigation will provide knowledge on best practices, frameworks, and policies that will facilitate trust-building within the digital space, guaranteeing sustainable development.

2.4. Research methods

The research employed a mixed approach combining qualitative review with quantitative analysis:

- *Literature Review:* Systematic examination of existing definitions, theories, and case studies to explore cybersecurity and digital trust interrelations. It is justified as it provides a theoretical foundation, synthesizing global definitions and frameworks (e. g., CIA triad) to contextualize Azerbaijan's challenges. This method is cost-effective and essential for identifying unaddressed empirical needs in developing economies like Azerbaijan, where large-scale surveys are resource-intensive.
- *Quantitative Survey Analysis:* Descriptive statistics on responses (e. g., percentages for awareness levels), followed by inferential statistics including Spearman rank correlation coefficients to assess relationships (e. g., between awareness and incidents). It is selected for its ability to gather real-world, Azerbaijan-specific data from a diverse sample (129 participants across sectors), enabling statistical validation of hypotheses (e. g., correlations between training and incidents). Spearman correlation was chosen over Pearson due to the ordinal nature of survey responses (e. g., awareness levels as "low/moderate/high"), ensuring non-parametric robustness for non-normal data. This method overcomes the limitations of theoretical studies [2] by providing numerical insights tailored to transitioning economies.
- *Risk Heatmap Modeling:* A visual risk assessment map based on respondent evaluations of threat likelihood and impact, categorized on a 1–3 scale (low to high). It is justified for its visual simplicity in communicating complex risks (e. g., high-impact threats like data breaches), aiding practical recommendations. It builds on survey data to prioritize interventions, aligning with risk management frameworks [50].
- *Comparative Analysis:* Benchmarking Azerbaijan's data against global trends (e. g., cybersecurity rankings) to highlight unique challenges. It is chosen to situate Azerbaijan's findings globally (e. g., vs. Japan or Algeria in Comparitech rankings), highlighting transferable best practices while accounting for local contexts like rapid digital growth outpacing regulations [3, 4].

This combination ensures a balanced, evidence-based approach: qualitative for depth, quantitative for objectivity, and comparative for broader applicability. Methods were sequenced to build progressively – theory informing survey design, survey data enabling analysis – while minimizing biases through anonymity and random sampling.

Data processing involved cleaning survey responses, computing correlations, and generating visualizations.

The methods were chosen to address the research gaps identified in the introduction: limited empirical data on Azerbaijan-specific cybersecurity practices and their impact on digital trust, as noted in prior studies [1–5], which are often theoretical or sector-limited.

All data collection, processing, and analysis were performed on a personal computer (standard laptop with Intel Core i7 processor, 16 GB RAM, and Windows 11 operating system) to ensure accessibility and replicability in a resource-constrained research environment.

Initial data entry and basic descriptive statistics used Microsoft Excel (version 2021) for its ease in handling survey responses. Advanced statistical analysis (e. g., correlations) employed SPSS (version 28) for its robust non-parametric tools. For detailed processing, visualization, and scripting, Python 3.12 was used with libraries including pandas (for data manipulation), scipy (for Spearman correlations), seaborn and matplotlib (for heatmaps and plots). This software suite was selected for compatibility: Excel/SPSS for user-friendly initial exploration, Python for scalable, reproducible advanced analytics.

The use of literature review, survey-based quantitative analysis, and comparative analysis in the text helps examine the dynamic

interaction between cyber-security practices and digital trust formation in Azerbaijan as well as elsewhere in the world.

An extensive review of existing literature was conducted to explore the foundational theories of cybersecurity and digital trust. This involved examining publications from academic circles, industry reports, and case studies from leading companies like Gartner, Accenture, PwC, and KPMG. The reviewed materials deepened understanding of critical concepts such as the significance of data protection, relevant privacy regulations (like General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), and the ethical utilization of data.

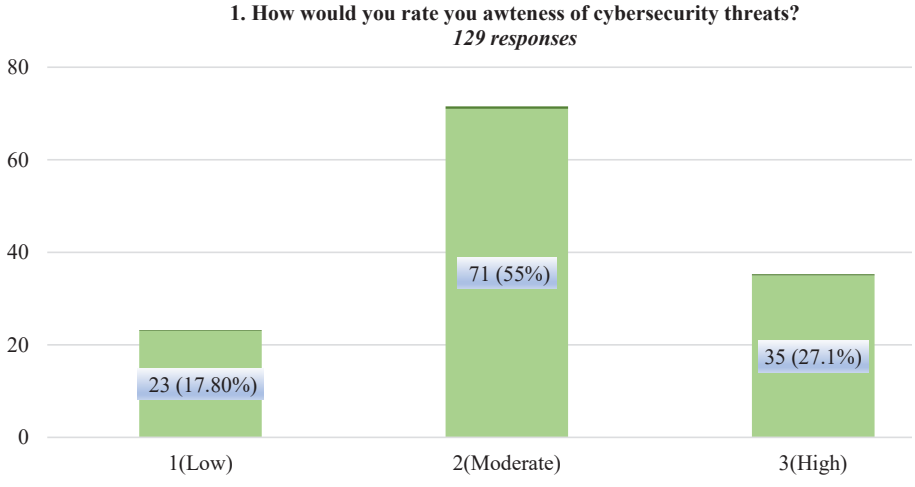

Fig. 6. Organizations' awareness of cybersecurity threats

Concurrently, case studies concerning cyber incidents, including ransomware attacks and other cyber threats, offered valuable perspectives on best practices.

Additionally, the article presents a comparative analysis of global cybersecurity practices. Data from various sources, including Statista and Comparitech, was utilized for this comparison.

Moreover, this report features an analysis based on a survey that enhances theoretical insights with a specific focus on organizations and individuals in Azerbaijan through quantitative methods. This research involved 129 participants from various fields, including finance, government agencies, and private companies.

The survey focused on several key aspects, including:

– awareness of cybersecurity threats within organizations;
– the adoption of security protocols like multi-factor authentication (MFA), encryption, firewalls, and training for employees;
– the frequency of cybersecurity incidents (such as data breaches, phishing scams, and fraud) over the last year;
– views on digital trust concerning online services, especially in banking and e-commerce;
– trust in Azerbaijan's legal systems to safeguard against cyber threats.

The survey results were analyzed using quantitative statistical approaches to detect trends and relationships between cybersecurity efforts and digital trust. Data processing was performed using Python 3.12, along with pandas, seaborn, and scipy libraries. The Spearman rank correlation coefficient was applied due to the ordinal nature of most responses. A risk assessment map was created based on respondents' evaluations of likelihood and impact. Visualization was executed using matplotlib and seaborn libraries.

3. Results and Discussion

3.1. Results

The author has created a survey named "Cybersecurity in Azerbaijan", which consists of 12 questions focusing on the most common cybersecurity problems. Among all the companies functioning in Azerbaijan, both local and international, 30 leading companies in different spheres including oil and gas sector have been chosen randomly and the survey has been distributed among employees of these companies by internal mails and social network platforms. The survey has been announced to be anonymous, and confidentiality of the responses has been guaranteed so that the participants feel free to respond the questionnaire using responses conforming to the truth.

According to the sample size calculation, 121 responses needed to be collected but in total 129 responses have been collected and analyzed. Fig. 6 illustrates organizations' awareness of cybersecurity threats.

With a population of 129 participants, the results show that there is a different degree of awareness existing with regard to cybersecurity threats. Low awareness was shown to be possessed by 23 participants, contributing about 17.8% of the entire population. Moderate awareness was shown by 71 participants, constituting about 55% of the entire population. Finally, high awareness was shown to be possessed by 35 participants, accounting for approximately 27.1% of the entire population. Therefore, the outcome of this analysis shows that more than half of the organizations exhibit moderate awareness, but only a quarter exhibit high awareness. However, this draws attention to the fact that more education, as well as policy formulation, might be necessary, especially within the low-awareness group, in order to improve their preparedness against cyber threats.

Fig. 7 illustrates presence of a dedicated cybersecurity team or specialist.

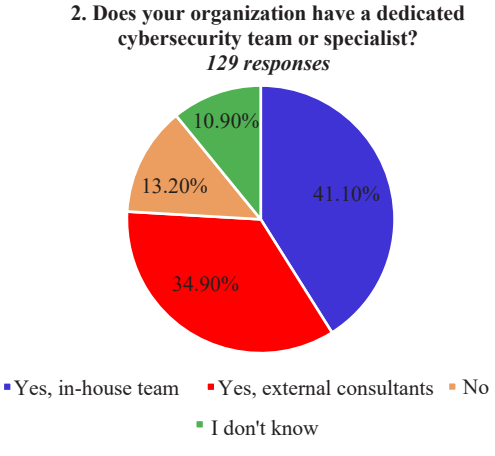

Fig. 7. Presence of a dedicated cybersecurity team or specialist

Of the total participants, 53 (41.1%) reported that their organizations possessed a cybersecurity team. This clearly shows that many organizations value the importance of being in charge of their cybersecurity. On the other hand, the services of external cybersecurity consultants were cited by 45 participants (34.9%). It can thus be seen that most individuals depend on experts outside their organizations in order to handle their cybersecurity. Meanwhile, 17 (13.2 percent) of the respondents reported that their organization lacks a cybersecurity team, which may pose a threat in terms of the focus that may not be placed on cybersecurity. Finally, 14 (10.9 percent) of the participants did not show any awareness, which may indicate a lack of knowledge of the

ISSN-L 2664-9969; E-ISSN 2706-5448

measures in place within their organizations on cybersecurity. Nearly all types of organizations appear to either employ their own in-house personnel or hire consultant experts for their cybersecurity. But the fact that some organizations remain unclear as to their in-house or cybersecurity structure accentuates that more attention must be devoted to cybersecurity awareness.

Fig. 8 presents frequency of cybersecurity training for employees.

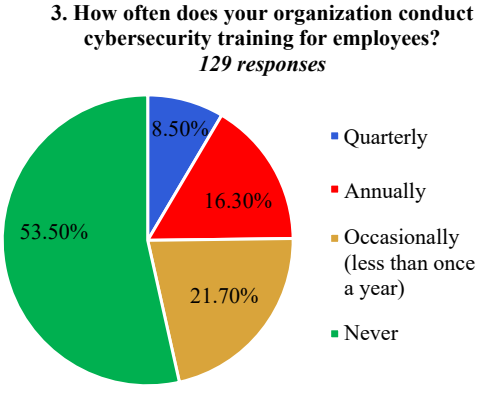

Fig. 8. Frequency of cybersecurity training for employees

Among the total number of participants surveyed, 69 (53.5%) reported that their organization never conducts cybersecurity trainings for employees, 28 (21.7%) reported that their organization conducts them occasionally, less than once a year, and 21 (16.3%) reported that their organization conducts them annually. Of the respondents, only 11 (8.5 percent) reported that their companies provide cybersecurity training every quarter. Apparently, most companies do not conduct the trainings or do so occasionally, as shown in the statistics. This accentuates the importance of organizations focusing on frequent cyber security training for better cyber threat resistance. Moreover, this highlights the importance of employees being aware of cyber threats, which can be achieved through such trainings.

Fig. 9 illustrates cybersecurity measures currently employed by organizations.

By analyzing the results, it is found that security audits being carried out in the organizations on a periodic basis is the most practiced measure with 110 participants reporting that their organizations do so. Antivirus or anti-malware tools come second, being used in 95 organizations. Firewalls come third, being used in 61 organizations, thus showing that many organizations focus on protecting their networks against unauthorized access. Encrypting sensitive information is practiced by 41 firms that, although showing some level of understanding of its importance, may still require improvement. Multi-factor authentication (MFA) is practiced by only 11 firms, showing a worrisome deficiency in sophisticated access control strategies, despite the necessity of MFA in further securing the entry process. Employee cyber-security awareness is carried out by 13 firms, showing the importance being given to human elements within cyber-security, despite employees being the weakest link in cybersecurity defenses. A minimum of 1 respondent identified that their organization did not use any of the above, with 10 others expressing unfamiliarity with their organization's use of cybersecurity practices. Although many organizations place a high value on the use of audits, as well as basic protection software, the deployment rate of more sophisticated tools, such as two-factor authentication solutions as well as employee education, remains low.

Fig. 10 presents perceived biggest cybersecurity threats in Azerbaijan.

According to the results, the concern with regard to cyber threats, as shown by the majority of participants, is the breach of data as well as the leakage of information, as 57 of the participants (44.2 percent) highlighted this as their concern. Others were cyber threats posed by ransomware or malware, highlighted by 24 participants (18.6 percent) as being a big threat. DDoS, or Denial of Service, was highlighted as a threat by 16 participants (12.4 percent). Phishing/social engineering assaults were cited as being identified by 12 participants (9.3 percent), thus stressing the continuous threat posed by such deceptive practices designed to dupe individuals into submitting sensitive information. Insider threats, such as that posed by employees or contractors, was mentioned as being identified by 10 participants (7.8 percent), thus focusing attention on the dangers posed by insiders with malicious aims. Finally, 10 of the respondents reported that they were not aware, showing some element of ignorance in regard to cyber threats. Looking through the results, it is apparent that Azerbaijan-based organizations are most concerned with data infringements, as well as ransomware, with fewer being concerned with phishing, as well as insider threats. This clearly relates to worldwide cybersecurity threats, with its own priorities.

Fig. 11 illustrates cybersecurity incidents in organizations over the past 12 months.

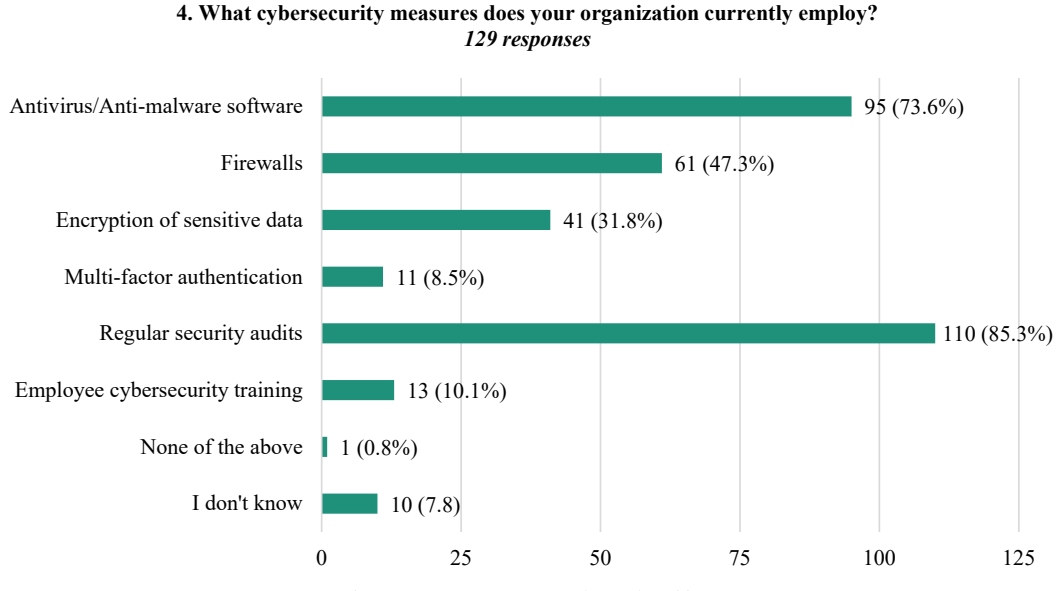

Fig. 9. Cybersecurity measures currently employed by organizations

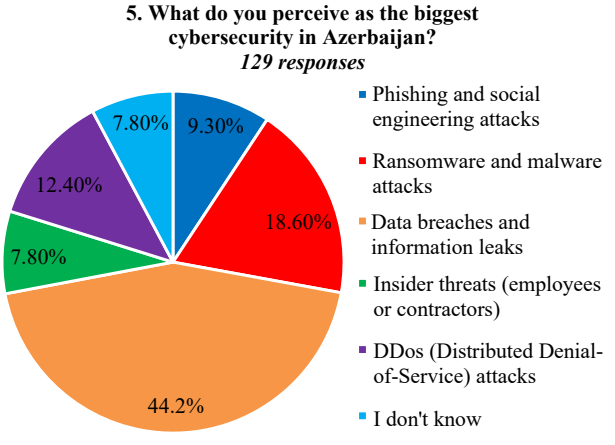

Fig. 10. Perceived biggest cybersecurity threats in Azerbaijan

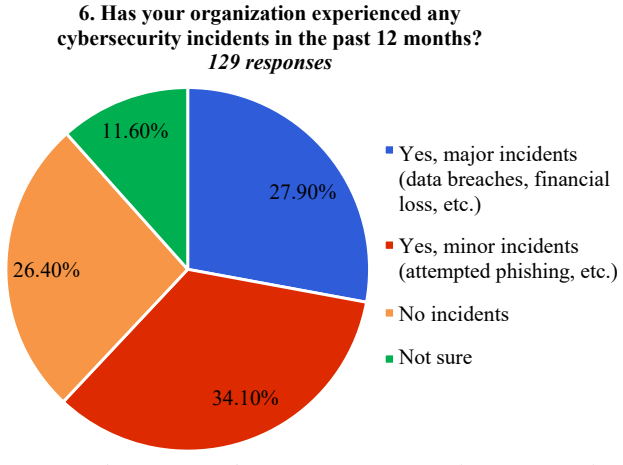

Fig. 11. Cybersecurity incidents in organizations over the past 12 months

Statistics show that 44 (34.1%) organizations experienced minor cyber events, for example, attempted phishing, compared to 36 (27.9%) that experienced serious events, for example, breach of data as well as financial losses. In the same percentage, 34 (26.4%) of the respondents mentioned that their organizations did not experience any cyber events within the last year. Although this is a positive finding, different levels of threat detection capacities within organizations might explain this. 15 respondents (11.6%) were not sure if their organizations had experienced any cybersecurity incidents. What emerges from the data is the fact that most of the organizations in Azerbaijan have been impacted by cyber security events. Whether big or small, such events occur with some frequency, and this explains why cyber security measures as well as employee awareness programs remain so essential in such regards.

Fig. 12 presents confidence in Azerbaijan's legal framework to protect against cyber threats.

The results of this survey indicate that there is a different level of confidence in Azerbaijan's legal system that provides cybersecurity protection. Most, that is, 77 respondents (60% of the whole number) did not give more than level 5, as this scale varies from level 1 to level 7, showing that the majority show moderate confidence in the existing laws. About 16% of the respondents, that is, 21, were confident with level 6, showing higher confidence in Azerbaijan's laws on cyber security. On the other hand, 14 participants (11%) gave a rate of 4, evaluating the system with some reservations. Less confident results were shown by 8 participants with rate level 3, 5 participants with rate level 2, and 2 participants with rate level 1, accounting for a total of 12.5% with low confidence concerning the cyber threat laws in Azerbaijan. Only 2 participants rated level 7, entirely confident with the system. Although a majority of participants express moderate to high levels of confidence in Azerbaijan's legal system as a whole with regard to cyber security, there still appears to be a measure of concern within this group. This would appear to provide Azerbaijan with the ideal opportunity to enhance its cyber security laws, as well as increase awareness, in order to gain more trust within its system.

Fig. 13 presents user perception of security when using online banking services in Azerbaijan.

What emerges clearly from this survey data is that most participants rate their feelings of security as being moderately safe with regard to Azerbaijan-based online banking services. Indeed, with regard to their perceptions of security, a full 83 participants (64.3 percent) rated their perceptions as being 4, clearly showing that they rated their perceptions of security as being relatively high. Likewise, a further 32 participants (24.8 percent) rated their perceptions of security as being 3, clearly showing that they rate their perceptions as being more neutral, that is, they rate their perceptions with caution. A relatively low number of participants, that is, 7 (5.4%), assessed their security at the highest level, that is, level 5, implying that they were perfectly confident in regard to the security of online banking services. At the lowest level, that is, level 2, were 5 participants (3.9%), while 2 participants (1.6%) assessed their security at level 1, implying that they were concerned about the security of online banking services.

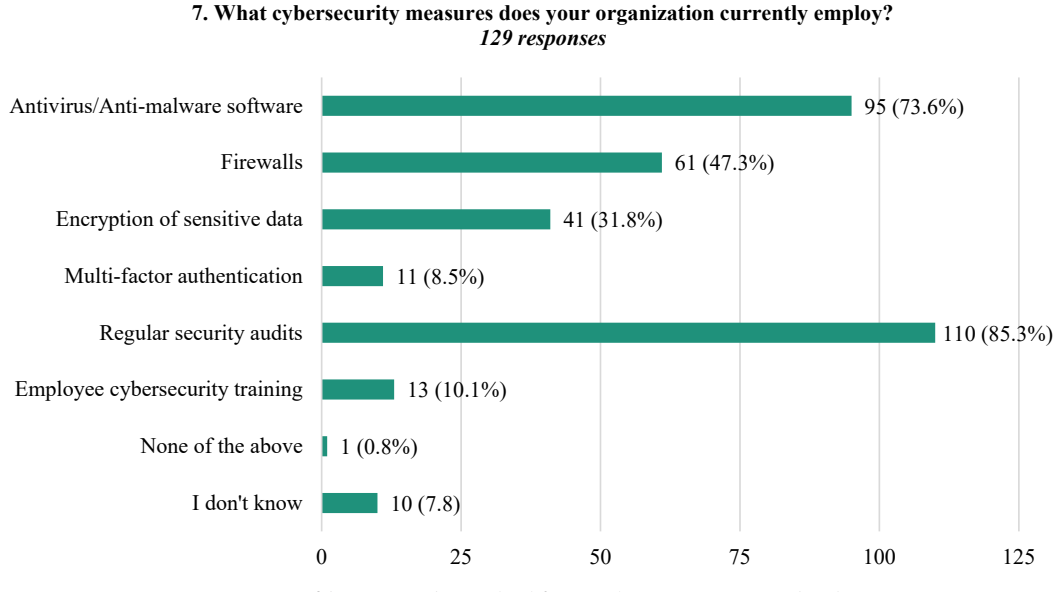

Fig. 12. Confidence in Azerbaijan's legal framework to protect against cyber threats

ISSN-L 2664-9969; E-ISSN 2706-5448

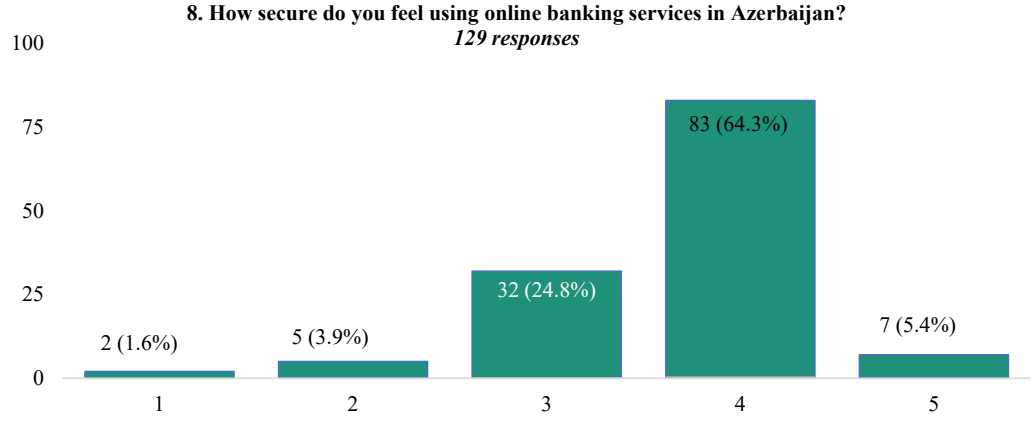

Fig. 13. User perception of security when using online banking services in Azerbaijan

What emerges from this data is that although most users in Azerbaijan feel safe with online banking facilities, there is still a significantly large group with a moderate or guarded approach, in addition to a smaller group that recognizes a great deal of risk. This points towards the importance of improved focus on security, transparency, as well as educating users on proper online banking practices.

Fig. 14 illustrates implementation of multi-factor authentication for online transactions by banks.

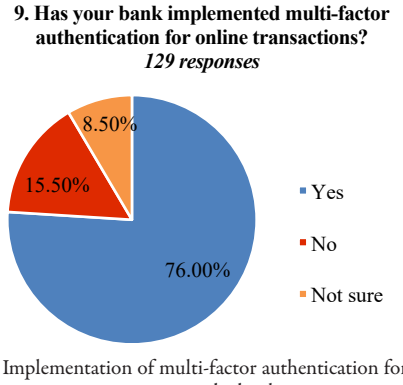

Fig. 14. Implementation of multi-factor authentication for online transactions by banks

From the results, it is evident that the majority of the respondents' banks use multi-factor authentication (MFA) for online transactions. A total of 98 (76%) of the participants' banks use MFA, thus exhibiting high levels of concern for the improvement of the safety measures of online banking services. However, the remaining 20 (15.5%) of the respondents claimed that their banks do not use MFA, thus demonstrating that some banking services still use conventional ways of securing online transactions. Moreover, a further 11 (8.5%) participants were unsure whether their bank utilizes MFA. Such a situation may indicate a deficiency in the bank's communications with regard to their security arrangements as well as a deficiency in the users' knowledge of the procedure. Indeed, the other positive note with regard to Azerbaijan's banking system is their extensive use of multi-factor authentication. However, the fact that there were some banks that do not use MFA, as well as some users being unsure of MFA usage, may indicate some weaknesses within the system.

Fig. 15 presents experience of fraudulent banking activities in the past year.

From the survey, there is evidence that 52 (40.3%) of the respondents experienced fraudulent banking practices within the previous year. However, 67 (51.9%) of the respondents did not experience any fraudulent banking practices. This shows that most organizations as well as individuals did not fall prey to banking fraud. However, the proximity of this figure to the other group shows that the banking industry still poses some dangers. Finally, 10 (7.8%) of the respondents were not sure whether they experienced fraudulent banking practices. The statistics show that there is a remarkable frequency of fraudulent banking practices, thus underlining the importance of proper security controls. Although more than half of the respondents did not fall prey to fraud, the fact that fraud did occur in such a high percentage of instances underlines the importance of fraud detection, fraud prevention, as well as educating users on fraud practices.

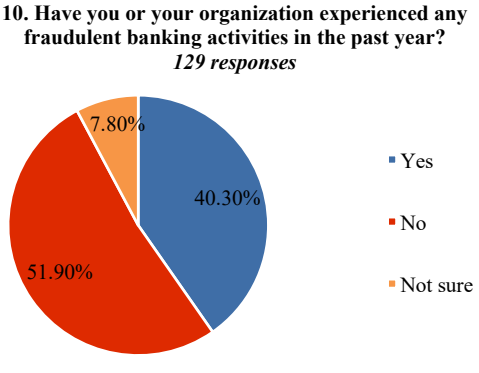

Fig. 15. Experience of fraudulent banking activities in the past year

Fig. 16 presents frequency of bank notifications on potential cybersecurity threats.

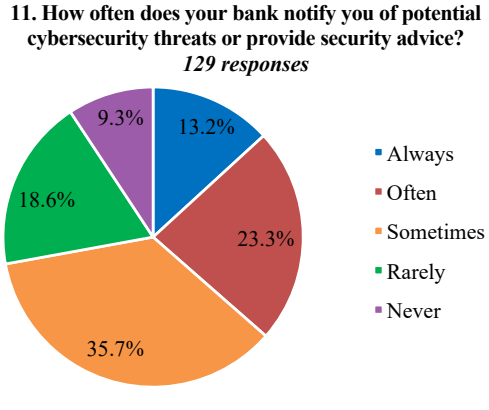

Fig. 16. Frequency of bank notifications on potential cybersecurity threats

The statistics indicate that some banks communicate with their clients more often than others through security warnings. A total of 46 participants (35.7 percent) reported that their banks often offer some

form of security warnings, though this is a moderate rate. On the other hand, 30 participants (23.3 percent) reported that their banks often communicate with them through warnings, with a further 17 (13.2 percent) reporting that their banks always do so. However, some banks rarely communicate with their clients, with 24 participants (18.6 percent) reporting this, while others do not communicate with them, with 12 (9.3 percent) reporting this. Although many banking institutions in Azerbaijan might offer occasional or periodic updates concerning cyber threats, there still remain a number of bank clients who do not often, if ever, hear such updates. Such a fact, however, represents a room for improvement with regard to the communications policy, thus allowing banking institutions to increase their clients' confidence in internet security practices.

Fig. 17 illustrates areas needing the most improvement in cybersecurity practices in Azerbaijan.

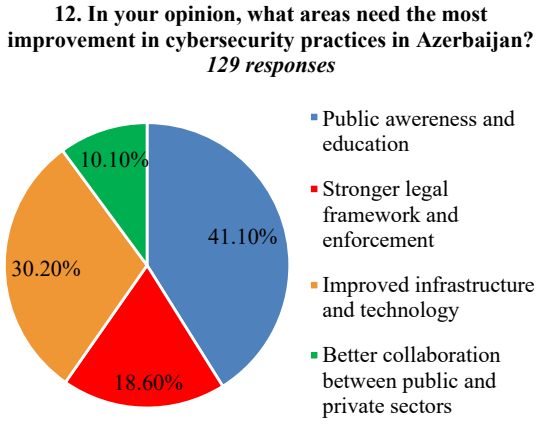

Fig. 17. Areas needing the most improvement in cybersecurity practices in Azerbaijan

However, the results of this survey show that public awareness as well as education stands out as the most pressing issues within the realm of cybersecurity that Azerbaijan must address. This was reflected in the views of 53 participants (41.1 percent) who considered this as their most urgent concern. This reflects the fact that a proper education campaign is necessary in order for people to be aware of cyber issues. Improving infrastructure, technology, addressing cyber issues through improved technology, was considered as the second most urgent concern, with 39 participants (30.2 percent). Enhanced legal frameworks and enforcement were recommended by 24 participants (18.6%). This reflects that although some legislation is being done, more powerful laws with strong enforcement measures would prevent cybercrimes as well as increase the resilience of the country's cyber defenses. Collaboration between the public and private sectors was recommended by 13 participants (10.1%). This reflects that if public-private partnerships work effectively, more cohesive cyber defense strategies will be realized. Indeed, the above results specify that there is a strong consensus on raising public awareness, as well as educating public users, on cyber security within Azerbaijan. However, technological advancement, changes in laws, as well as enhanced public-private partnerships, are some of the key elements that must be involved in the development of a strong cybersecurity system.

Based on the survey, some additional analyses were carried out with the purpose of better understanding the topic of cyber-security in Azerbaijan.

First, correlation analysis is carried out between awareness of cyber issues and cyber events. This helps in determining if there is any correlation within which organizations that demonstrate higher levels of cyber security awareness experience fewer key cyber events. The correlation value between cybersecurity awareness and incident occurrences is –0.33 with a value of 0.0001. There is a negative correlation of –0.33, showing that as levels of awareness increase, the number of incidents decreases. As organizational awareness rises, the chances of occurrence as well as its consequences will reduce. However, with a "*p*" value of 0.0001, this correlation is statistically significant, as the likelihood of this correlation being random is highly unlikely (Fig. 18).

The scatter plot in Fig. 18 visualizes the correlation between cybersecurity awareness levels and incident severity. The regression line indicates a negative relationship, where higher awareness levels (moving from Low to High on the *x*-axis) are associated with fewer or less severe incidents (moving from Major to None on the *y*-axis). Low awareness organizations are clustered towards higher incident severity, including major and minor incidents. With increasing awareness that reaches moderate and high levels, events transition towards less severe events, with many organizations facing either shallow events or no events. This corresponds with the finding that a strong positive association between cybersecurity awareness measures and low-level cybersecurity incident occurrence.

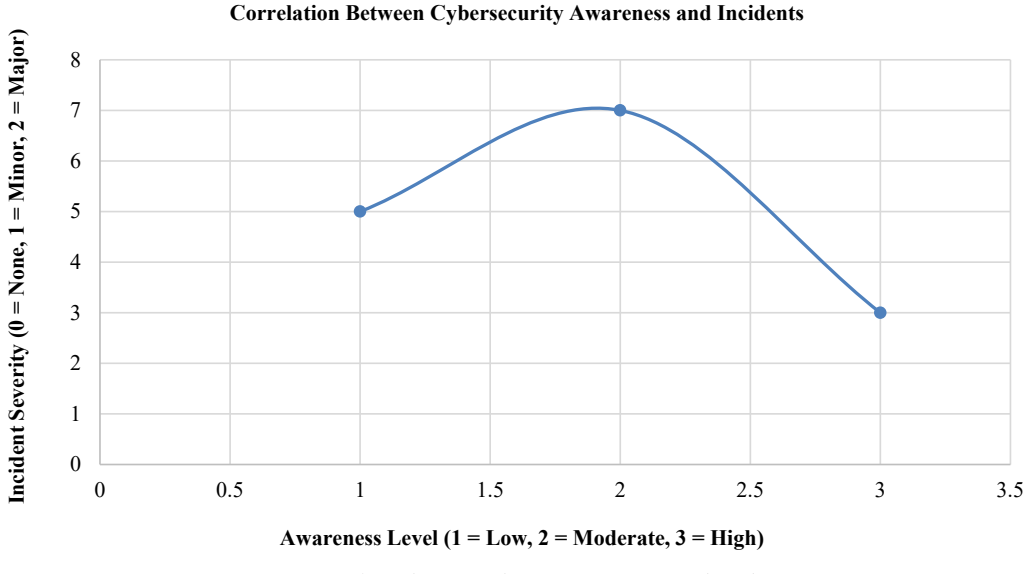

Fig. 18. Correlation between cybersecurity awareness and incidents

ISSN-L 2664-9969; E-ISSN 2706-5448

Then correlation analysis has been implemented for link between training frequency and security incidents. The Spearman correlation value for the frequency of cybersecurity training and the occurrence of cybersecurity incidents is –0.29 with a "*p*" value of 0.00087. A negative correlation value of –0.29 shows that with more frequent cybersecurity trainings, fewer or less severe cybersecurity incidents occur. With more frequent trainings (from *"Never" to "Quarterly"*), the likelihood/severity of cybersecurity incidents reduces. The *p*-value of 0.00087 suggests that this correlation is statistically significant, meaning there is a strong likelihood that the observed relationship is not due to random chance. So, organizations that provide regular cybersecurity training experience fewer and less severe incidents. This underscores the importance of consistent employee training programs in strengthening organizational defenses against cyber threats.

Lastly, correlation between MFA implementation and fraud prevention gas been carried out. The Spearman correlation coefficient between MFA implementation and fraud prevention is 0.3446, with a *p*-value of 0.000064. There is a positive correlation value (0.3446) that shows that as the implementation level of MFA (multi-factor authentication) increases, the instances of fraudulent banking activity reduce. This establishes that MFA is a powerful tool that protects against fraud. However, there is a low probability value (0.000064) that shows that this correlation can happen as a result of random chance, as the value is statistically significant. This strengthens the confidence in the conclusion that MFA plays a mandatory role in mitigating fraud.

In the next stage of analysis, risk assessment mapping has been formulated using survey results. Fig. 19 illustrates heatmap visually representing the risk assessment mapping for cybersecurity in Azerbaijan.

High likelihood/high impact risks (3.3), such as data breach, cyber security training, and banking fraud, are shown in the darkest shades of red, which indicate that they are critical. Medium risks, such as DDoS attack, unimplemented MFA, as well as gaps in public awareness, appear in the lighter shades of red, as they may be considered important but not as urgent. Lower likelihood risks, such as insider threats, may still inflict high impact on the heatmap, depicting that such events may inflict severe harm even if they happen with low likelihood.

3.2. Discussion

The survey found that Azerbaijan's awareness of cybersecurity is average: 55% of organizations have an average level, 27.1% have a high level, and 17.8% have a low level (Fig. 6). 53.5% of businesses don't train their workers on cybersecurity, and only 8.5% do so every three months (Fig. 8).

When it comes to safety, 85% of people check their security regularly, and 74% use antivirus software. But the answers show that only 76% of banks use multi-factor authentication and only 10% of organizations focus on training their workers (Fig. 9).

40.3% of the people who answered said they had seen fake banking activity in the last year. This is surprising because 76% of people use multi-factor authentication (MFA), which means that social engineering is a problem and users don't know how to use it (Fig. 15).

Statistical analysis demonstrated significant correlations between:

- level of knowledge and number of incidents: $r = -0.33$, $p = 0.0001$;
- frequency of training and number of incidents: $r = -0.29$, $p = 0.00087$;
- implementation of MFA and fraud reduction: $r = +0.3446$, $p = 0.000064$.

Fig. 19 is a risk heat map that shows three big risks: data breaches, not getting enough training, and making fake transactions. These are likely to happen and have a big impact.

Practical value. The results have a direct impact on practice: The State Department of Special Communications and Information Security of Azerbaijan says that national awareness campaigns and mandatory certification of state officials should be at the top of the list of things to do; They confirm that banks need to use mandatory MFA and One-Time Password (OTP tokens and do regular simulated fraud tests, which can cut down on fraud by 30–40% based on correlation data. You can quickly see how safe your computer is and choose what to do first (training and setting up MFA).

Research restrictions:

1. The sample of 129 people doesn't include everyone because there aren't enough people from the country.
2. You might think you can do more than you really can when you look at yourself.
3. This research is based on what will happen in January 2025. The threat landscape is changing quickly, so it needs to be updated a lot.

Prospects for further research. Conduct another survey in 2027–2028 to assess changes. Make sure that people from different areas are included in the sample of 400 people. Check out the results and see how they stack up against the results from the field studies in Georgia and Armenia. It is also possible to look into how AI-based security systems affect people's trust in digital systems.

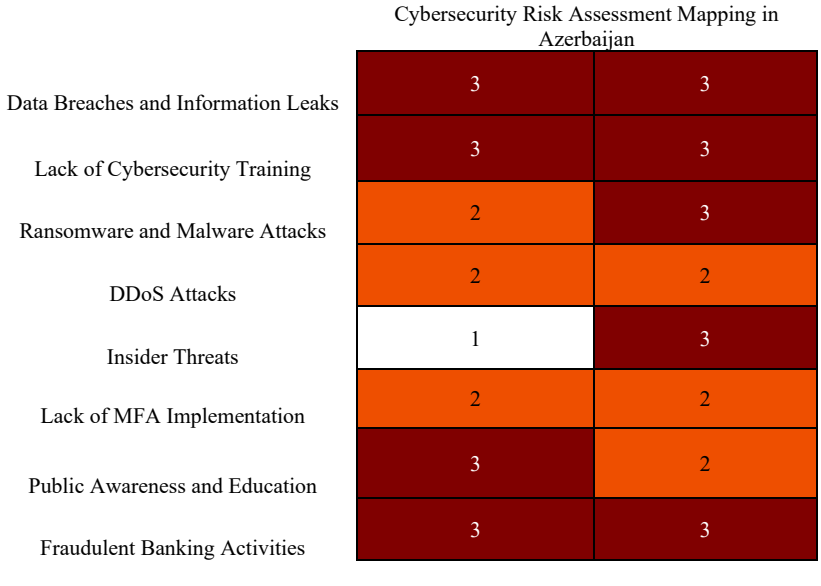

Fig. 19. Cybersecurity risk assessment mapping in Azerbaijan

4. Conclusions

1. A theoretical analysis of "cybersecurity" and "digital trust", as well as their interrelations, posits that cybersecurity is fundamental to the concept of digital trust. People's views on the safety, morality, and dependability of digital services are directly influenced by security measures that people can trust, such as regular staff training and the widespread use of multi-factor authentication. Cybersecurity is also very important because new tools and services can make people less trusting of the internet.

2. A survey of people from different fields in Azerbaijan found that these groups were only somewhat aware of cyber security; 55% of those who answered said this was the case. Moderately, 17.8% Low; participants also said that employee training is not common at all – 53.5% of organizations do not do it. The survey also showed that the people who answered it didn't trust digital technology very much. Only 5.4% of users rated their online banking security a perfect 5 out of 5, while 64.3% rated it a 4 out of 5, which is average.

3. A statistical analysis of the survey results found several relationships that were statistically significant. For instance, the level of awareness of an issue and how often/seriously it happened had a negative Spearman correlation value of (–0.33) and a p-value of (< 0.0001); the frequency of training received for an issue and how often/seriously it happened also had a negative Spearman correlation value (–0.29) and p-value (< 0.00087); and the degree of multifactor authentication (MFA) implementation and the reduction in fraudulent banking transactions had a positive Spearman correlation value (+0.3446) and p-value (< 0.000064). The actions taken to address Azerbaijan's rapidly digitalizing economy have been very effective, as the results demonstrate.

4. Based on the data that was gathered, a list of prioritized practical suggestions was made. These included mandatory quarterly cybersecurity training for employees in the state and banking sectors, moving all financial transactions to multi-factor authentication that uses hardware or biometric components, annual independent audits, and large national campaigns to raise public awareness. If everyone follows these steps all the time, fake transactions should go down by at least 35–40%, and people and businesses should trust the internet much more in 2–3 years.

Conflicts of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The research was performed without financial support.

Data availability

Data will be made available on reasonable request.

Use of artificial intelligence

During the preparation of the manuscript, the artificial intelligence tools ChatGPT (version GPT-4o, OpenAI, 2024) and Deep-Seek-V3 (DeepSeek, 2024) were utilised solely as supplementary instruments for language editing and the elucidation of formulations. The authors bear complete responsibility for the content, reliability, and scientific integrity of the material presented. These instruments were not employed to gather or produce empirical data, perform statistical analyses, or establish the conceptual frameworks of research.

Declaration submitted by: Khayala Alasgarova.

Authors' contributions

Khayala Alasgarova: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review and editing, Visualization, Supervision, Project administration; ***Sahib Ramazanov***: Conceptualization, Supervision, Validation, Resources, Writing – review and editing.

References

1. Maurer, T., Morgus, R. (2014). Compilation of existing cybersecurity and information security related definitions. *New America*. Available at: https://static.newamerica.org/attachments/175-compilation-of-existing-cybersecurity-and-information-security-related-definitions/OTI_Compilation_of_Existing_Cybersecurity_and_Information_Security_Related_Definitions_Updated122015.pdf
2. Hao, X., Li, Y., Ren, S., Wu, H., Hao, Y. (2023). The role of digitalization on green economic growth: Does industrial structure optimization and green innovation matter? *Journal of Environmental Management, 325*, 116504. https://doi.org/10.1016/j.jenvman.2022.116504
3. Kluiters, L., Srivastava, M., Tyll, L. (2022). The impact of digital trust on firm value and governance: an empirical investigation of US firms. *Society and Business Review, 18 (1),* 71–103. https://doi.org/10.1108/sbr-07-2021-0119
4. Uchendu, B., Nurse, J. R. C., Bada, M., Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109,* 102387. https://doi.org/10.1016/j.cose.2021.102387
5. Shikhaliyev, R. (2023). Cybersecurity analysis of industrial control systems. *Problems of Information Society, 14 (2),* 47–54. https://doi.org/10.25045/jpis.v14.i2.06
6. Manjikian, M. (2017). *Cybersecurity Ethics*. Routledge, 246. https://doi.org/10.4324/9781315196275
7. Kostopoulos, G. K. (2017). *Cyberspace and cybersecurity*. Auerbach Publications. https://doi.org/10.1201/9781315116488
8. Veríssimo, P., Rodrigues, L. (2001). Fundamental Security Concepts. *Distributed Systems for System Architects*. Boston: Springer, 377–393. https://doi.org/10.1007/978-1-4615-1663-7_16
9. Kim, L.; Hübner, U. H., Mustata Wilson, G., Morawski, T. S., Ball, M. J. (Eds.) (2022). Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information. *Nursing Informatics*. Cham: Springer, 391–410. https://doi.org/10.1007/978-3-030-91237-6_26
10. Shah, S. S., Shah, S. A. H. (2024). Trust as a determinant of social welfare in the digital economy. *Social Network Analysis and Mining, 14 (1)*. https://doi.org/10.1007/s13278-024-01238-5
11. Herath, S. K., Herath, L. M., Yoo, J. K. (2024). Opportunities and Challenges of Digital Audits and Compliance. *Impact of Digitalization on Reporting, Tax Avoidance, Accounting, and Green Finance*, 1–35. https://doi.org/10.4018/979-8-3693-1678-8.ch001
12. Ablyazov, T., Asaturova, J., Koscheyev, V. (2018). Digital technologies: new forms and tools of business activity. *SHS Web of Conferences, 44*, 00004. https://doi.org/10.1051/shsconf/20184400004
13. Osburg, T. (2019). Changing Relevance of Trust in Digital Worlds. *Media Trust in a Digital World*, 15–33. https://doi.org/10.1007/978-3-030-30774-5_2
14. Huda, M. (2023). Trust as a key element for quality communication and information management: insights into developing safe cyber-organisational sustainability. *International Journal of Organizational Analysis, 32 (8),* 1539–1558. https://doi.org/10.1108/ijoa-12-2022-3532
15. Guo, Y. (2022). Digital Trust and the Reconstruction of Trust in the Digital Society: An Integrated Model based on Trust Theory and Expectation Confirmation Theory. *Digital Government: Research and Practice, 3 (4),* 1–19. https://doi.org/10.1145/3543860
16. *PwC UK*. Available at: https://www.pwc.co.uk Last accessed: 09.01.2025.
17. Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce, 23 (2),* 1–11. Available at: https://www.icommercecentral.com/open-access/impact-of-cyberattacks-on-financial-institutions.pdf
18. Rezaei, F. (2019). Iran's Military Capability: The Structure and Strength of Forces. *Insight Turkey, 21 (4),* 183–216. Available at: https://www.insightturkey.com/articles/irans-military-capability-the-structure-and-strength-of-forces
19. Berglyd, K. J. T. (2022). *Strategic Culture and State Behaviour in Cyberspace: How Iran's Strategic Culture Influences its Behaviour in Cyberspace*. [Master's Thesis]. Available at: https://www.duo.uio.no/bitstream/handle/10852/96599/1/STV4992-Master-s-Thesis-Knut-Joachim-Tander–Berglyd-Spring-2022.pdf
20. Perwej, Dr. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management, 9 (12),* 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

ISSN-L 2664-9969; E-ISSN 2706-5448

21. Saleh, M. E., Aly, A. A., Omara, F. A. (2016). Data Security Using Cryptography and Steganography Techniques. *International Journal of Advanced Computer Science and Applications, 7 (6).* https://doi.org/10.14569/ijacsa.2016.070651
22. Chio, C., Freeman, D. (2018). *Machine learning and security: Protecting systems with data and algorithms.* O'Reilly Media, 383. Available at: https://virtualmmx.ddns.net/gbooks/MachineLearningandSecurity.pdf
23. Carr, M., Shahandashti, S. F.; Hölbl, M., Rannenberg, K., Welzer, T. (Eds.) (2020). Revisiting Security Vulnerabilities in Commercial Password Managers. *ICT Systems Security and Privacy Protection.* Cham: Springer, 265–279. https://doi.org/10.1007/978-3-030-58201-2_18
24. Stobert, E., Biddle, R. (2018). The Password Life Cycle. *ACM Transactions on Privacy and Security, 21 (3),* 1–32. https://doi.org/10.1145/3183341
25. Rizvi, S., Orr, R., Cox, A., Ashokkumar, P., Rizvi, M. R. (2020). Identifying the attack surface for IoT network. *Internet of Things, 9,* 100162. https://doi.org/10.1016/j.iot.2020.100162
26. Borky, J. M., Bradley, T. H. (2019). Protecting Information with Cybersecurity. *Effective Model-Based Systems Engineering.* Cham: Springer, 345–404. https://doi.org/10.1007/978-3-319-95669-5_10
27. Michael, K., Kobran, S., Abbas, R., Hamdoun, S. (2019). Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals. *2019 IEEE International Symposium on Technology and Society (ISTAS).* https://doi.org/10.1109/istas48451.2019.8937956
28. Chitadze, N. (2023). Basic Principles of Information and Cyber Security. *Analyzing New Forms of Social Disorders in Modern Virtual Environments,* 193–223. https://doi.org/10.4018/978-1-6684-5760-3.ch009
29. Lundgren, B., Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics, 25 (2),* 419–441. https://doi.org/10.1007/s11948-017-9992-1
30. Villalón-Fonseca, R. (2022). The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity. *Computers & Security,* 120, 102805. https://doi.org/10.1016/j.cose.2022.102805
31. Saber, J. A. (2016). *Determining small business cybersecurity strategies to prevent data breaches.* [Doctoral dissertation; Walden University]. Available at: https://scholarworks.waldenu.edu/dissertations/4991/
32. Razikin, K., Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal, 23 (3),* 383–404. https://doi.org/10.1016/j.eij.2022.03.001
33. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. *Computer Science & IT Research Journal, 5 (1),* 1–25. https://doi.org/10.51594/csitrj.v5i1.699
34. Priyadarshini, I.; Le, D., Kumar, R., Mishra, B. K., Khari, M., Chatterjee, J. M. (Eds.) (2019). Introduction on cybersecurity. *Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies,* 1–37. https://doi.org/10.1002/9781119488330
35. Astani, M., Ready, K. J. (2016). Trends and preventive strategies for mitigating cybersecurity breaches in organizations. *Issues in Information Systems, 17 (2).* https://doi.org/10.48009/2_iis_2016_208-214
36. Paleri, P. (2022). *Revisiting National Security: Prospecting Governance for Human Well-Being.* Singapore: Springer. https://doi.org/10.1007/978-981-16-8293-3
37. Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science, 215,* 483–487. https://doi.org/10.1016/j.procs.2022.12.050
38. Mishra, A. (2022). *Modern Cybersecurity Strategies for Enterprises: Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods.* BPB Publications, 564. Available at: https://bpbonline.com/products/modern-cybersecurity-strategies-for-enterprises
39. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B. et al. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation.* arXiv. https://doi.org/10.48550/arXiv.1802.07228
40. Alexei, A., Alexei, A. (2023). The difference between cyber security vs information security. *Journal of Engineering Science, 29 (4),* 72–83. https://doi.org/10.52326/jes.utm.2022.29(4).08
41. Safitra, M. F., Lubis, M., Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability, 15 (18),* 13369. https://doi.org/10.3390/su151813369
42. Ahmed, S., Khan, M. (2023). Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem. *AI, IoT and the Fourth Industrial Revolution Review*, *13* (9), 1–17. Available at: https://ru.scribd.com/document/798142114/Securing-the-Internet-of-Things?utm_source
43. Al Hayajneh, A., Thakur, H. N., Thakur, K. (2023). The Evolution of Information Security Strategies: A Comprehensive Investigation of INFOSEC Risk Assessment in the Contemporary Information Era. *Computer and Information Science, 16 (4).* https://doi.org/10.5539/cis.v16n4p1
44. Manning, E. (2023). *Optimizing Incident Management Processes for Effective Cybersecurity Incident Response.* [Master's thesis; National College of Ireland]. Available at: https://norma.ncirl.ie/7296/
45. Manoharan, A., Sarker, M. (2022). Revolutionizing cybersecurity: unleashing the power of artificial intelligence and machine learning for nextgeneration threat detection. *International Research Journal of Modernization in Engineering Technology & Science, 4 (12).* https://doi.org/10.56726/irjmets32644
46. Salem, A. H., Azzam, S. M., Emam, O. E., Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11 (1).* https://doi.org/10.1186/s40537-024-00957-y
47. Tar, S. J. (2024). *Factors That Influence Cybersecurity Risk Management Within the Department of Homeland Security.* [Doctoral dissertation; Capitol Technology University].
48. Stine, K., Quinn, S., Witte, G., Gardner, R. K. (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM).* National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8286
49. Loi, M., Christen, M. (2020). Ethical Frameworks for Cybersecurity. *The Ethics of Cybersecurity,* 73–95. https://doi.org/10.1007/978-3-030-29053-5_4
50. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D. et al. (2017). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis, 40 (1),* 183–199. https://doi.org/10.1111/risa.12891
51. Cardona, L. A. L. (2021). Technological trends. *Ingeniería Solidaria, 17 (1),* 1–28. https://doi.org/10.16925/2357-6014.2021.01.02
52. Gangwar, S., Narang, V. (2022). A Survey on Emerging Cyber Crimes and Their Impact Worldwide. *Research Anthology on Combating Cyber-Aggression and Online Negativity.* IGI Global Scientific Publishing, 1583–1595. https://doi.org/10.4018/978-1-6684-5594-4.ch080
53. Allende López, M., Da Silva, M. M. (2019). *Quantum Technologies: Digital Transformation, Social Impact, and Cross-sector Disruption.* Inter-American Development Bank. https://doi.org/10.18235/0001613
54. Fukushima, A. (2021). *Promises and challenges of digital connectivity.* European University Institute. Available at: https://cadmus.eui.eu/entities/publication/e9f6e26a-af6f-514f-8e9e-a36f99888c18
55. *Source: Statista 2023.* ResearchGate. Available at: https://www.researchgate.net/figure/Source-Statista-2023_fig1_373775351
56. Uma, M., Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security, 15 (5),* 390–396. Available at: http://ijns.jalaxy.com.tw/contents/ijns-v15-n5/ijns-2013-v15-n5-p390-396.pdf

✉ ***Khayala Alasgarova,*** *PhD, Assistant, Department of Economics and Business, Azerbaijan State University of Economics (UNEC), Baku, Azerbaijan, e-mail: khayala.alasgarova@unec.edu.az, ORCID: https://orcid.org/0009-0003-8489-2025*

Sahib Ramazanov, *PhD, Assistant Professor, Department of Economics and Business, Azerbaijan State University of Economics (UNEC), Baku, Azerbaijan, ORCID: https://orcid.org/0000-0003-2582-3188*

✉ *Corresponding author*