



Akademik Eğitim ve Sosyal Bilimler Dergisi (AJESS Journal)

Cybersecurity as a mechanism to ensure the success of digital transformation

Dr. Ahmed Sayah salih, Hassiba Ben Bouali University of Chlef , Algeria
s.ahmedsayah@univ-chlef.dz

Dr. Kebaili Dahbia, Hassiba Ben Bouali University of Chlef , Algeria.
d.kebaili@univ-chlef.dz

Article History

Received : 31/07/2026 ; Accepted : 23/08/2026 ; Published : 26/08/2026

Abstract

This study aims to highlight the role of cybersecurity in ensuring the success of digital transformation within organizations, as it is a fundamental element for protecting digital systems and data from various cyber threats and attacks. The study also sheds light on the complementary relationship between cybersecurity and digital transformation, as the success of digitization is linked to the effectiveness of the adopted protection measures.

The study adopted a descriptive-analytical approach to analyze the concepts of cybersecurity and digital transformation, addressing the most prominent cybersecurity challenges facing modern organizations. The study concluded that cybersecurity contributes to enhancing digital trust, protecting information, and ensuring the continuity of electronic services, making it a fundamental pillar for achieving a secure and effective digital transformation.

Keywords: Cybersecurity, Digital Transformation, Digital Security, Data Protection, Cyber Attacks, Information Systems

Introduction:

The world has witnessed a massive technological revolution in recent decades, leading to the transition of societies and institutions from traditional to digital systems. This phenomenon, known as digital transformation, has become a strategic necessity for achieving efficiency, speed, and improved service quality. This transformation has contributed to radical changes in various sectors, such as administration, education, health, the economy, and communications, making digital technology a fundamental pillar of modern development.

However, this rapid expansion in the use of digital technology has been accompanied by a significant increase in cyber risks and threats, such as cyberattacks, system breaches, data theft, and digital espionage. This has made cybersecurity one of the most important challenges facing institutions and countries in the digital age.

Cybersecurity is now a fundamental mechanism for ensuring the success of digital transformation projects by protecting information systems, securing data, guaranteeing the continuity of digital services, and enhancing user trust in the digital environment.

Importance of the Study:

The importance of this study lies in highlighting the pivotal role of cybersecurity in protecting digital institutions and ensuring the success of digital transformation projects, in addition to clarifying the most important challenges and modern mechanisms adopted to achieve information security.

Study Objectives:

- To understand the concepts of cybersecurity and digital transformation.
- To highlight the relationship between cybersecurity and digital transformation.
- To analyze the most significant cyber threats facing organizations.
- To examine mechanisms for enhancing cybersecurity to ensure the success of digital transformation.

Study Hypotheses :

- Cybersecurity effectively contributes to the success of digital transformation.
- The higher the level of cybersecurity, the more efficient digital services will be.
- Weak cybersecurity hinders digital transformation projects.

Research Problem:**Main Problem:**

To what extent does cybersecurity contribute to ensuring the success of digital transformation and protecting organizations from digital risks and threats?

Sub-questions

- 1 .What is meant by cybersecurity and digital transformation?
- 2 .What are the most prominent cyber threats facing digital organizations?
- 3 .How does cybersecurity contribute to enhancing the success of digital transformation?
- 4 .What are the most important mechanisms and strategies adopted to achieve cyber protection?

Research Methodology

- Descriptive-analytical approach.
- Comparative approach used when needed.

Section 1: The Conceptual Framework of Cybersecurity and Digital Transformation

The rapid pace of technological development has led to the widespread use of digital technologies across various organizations, contributing to the emergence of digital transformation as a means to improve performance and develop services. However, this transformation has been accompanied by an increase in cyber threats and risks, making cybersecurity a fundamental element for protecting systems and data and ensuring the continuity of digital services.

Therefore, this section aims to clarify the basic concepts related to cybersecurity and digital transformation, highlighting their most important characteristics, objectives, and the relationship between them.

Requirement 1: The Nature of Cybersecurity

Cybersecurity has become one of the most important pillars in the modern digital environment, given the increasing reliance on electronic systems and the growing number of cyber threats and attacks. It aims to protect information, data, and digital systems from various risks that may threaten their security and integrity. Accordingly, this requirement will address the concept of cybersecurity, its objectives, and the most prominent threats it faces.

Section 1: The Concept of Cybersecurity

Cybersecurity is a modern concept that emerged with technological advancements and the increasing reliance on digital systems. It has become essential for protecting information and data from various cyber threats. Cybersecurity focuses on providing protection for systems and networks, ensuring the security of the digital environment, and guaranteeing the continuity of its services.

Definition of Cybersecurity

Cybersecurity is defined as the set of means, technologies, and procedures aimed at protecting information systems, networks, devices, and data from cyberattacks and breaches, ensuring the confidentiality and integrity of information, and the continuity of digital services¹.

Emergence and Development of Cybersecurity

Cybersecurity emerged with the beginning of the use of computers and electronic networks. However, its development is closely linked to the spread of the internet and the expansion of digital technology use. With the increasing reliance on electronic systems and the emergence of cybercrimes, cybersecurity has become a necessary field for protecting information and digital infrastructure. It has witnessed remarkable development through the adoption of modern technologies such as encryption, artificial intelligence, and intrusion detection systems.²

Cybersecurity Characteristics³

- Protecting the confidentiality of information and preventing unauthorized access.
- Ensuring data integrity and preventing tampering.
- Maintaining the continuity of digital systems and services.
 - The ability to counter cyber threats and attacks.
 - Relying on modern technologies and continuous updates to address evolving digital risks.

Section Two: Cybersecurity Objectives**1 .Data Protection**

Cybersecurity aims to protect data and information from theft, alteration, or destruction by using modern methods and technologies that ensure its security within digital systems.⁴

2 .Ensuring Information Confidentiality

¹ Ahmed Al-Hadi Al-Husseini, *Electronic Administration and the Challenges of Digital Transformation*, (Algeria: Dar Al-Khaldounia, 2021), p. 44.

² Nasser Dadi Addoun, *Public Administration and Modern Transformations*, (Algeria: Dar Al-Muhammadiyah, 2020), p. 174.

³ Ahmed Yousef, *Information Security and Cyberspace*, *Dar Al-Fikr Al-Jami'i*, Cairo, 2022, p. 88.

⁴ Sami Abdul Karim, *Digital Security and Information Protection*, (Amman: Dar Al-Bidaya, 2021), p. 63.

Cybersecurity aims to maintain the confidentiality of information and prevent unauthorized access to it, especially sensitive information related to organizations or individuals¹.

3 .Integrity of Digital Systems

Cybersecurity works to protect digital systems and networks from breaches and cyberattacks, ensuring their integrity and efficiency in performing their functions².

4 .Continuity of Electronic Services

Cybersecurity contributes to ensuring the continuity of digital services and preventing their interruption due to attacks or technical malfunctions, thus enhancing user confidence in the digital environment³.

Section Three: Types of Cyber Threats

Cyber Intrusions

Cyber intrusions consist of attempts to gain unauthorized access to digital systems or networks with the aim of stealing information, manipulating data, or disrupting electronic services⁴.

Malware

Malicious software is designed to harm devices and information systems, such as viruses, spyware, and ransomware, leading to system disruptions or data theft.⁵

• Phishing

Phishing is one of the most widespread cybercrimes. It involves deceiving users through fake messages or websites to obtain personal information or banking details.

•Denial-of-Service (DoS) Attacks

DDoS attacks involve flooding servers or websites with a large number of requests, causing service disruptions and preventing users from accessing them.⁶

Data Theft

Data theft occurs when sensitive information, such as personal, financial, or confidential organizational data, is illegally obtained, potentially causing significant material and reputational losses⁷.

Second Requirement : The Nature of Digital Transformation

Digital transformation has become one of the most prominent modern trends adopted by organizations to improve performance and develop services using digital technology. This transformation has contributed to fundamental changes in work methods, communication, and service delivery, making it an essential element for achieving efficiency, speed, and innovation in various fields. Therefore, this section will address the concept of digital transformation, its objectives, and its most important areas.

First Section: The Concept of Digital Transformation

Definition of Digital Transformation

Digital transformation is defined as the process by which organizations move from traditional methods to using modern digital technologies in conducting⁸ business and providing services, with the aim of improving performance, increasing efficiency, and achieving speed and flexibility in operations.

Stages of Digital Transformation

Digital transformation goes through several essential stages, beginning with providing the technological infrastructure, then digitizing data and administrative processes, followed by employing digital systems and applications, culminating in the development of electronic services and achieving digital integration within the organization. Characteristics of the Digital Environment⁹

The digital environment is characterized by the rapid exchange of information, ease of communication, reliance on modern technology, flexibility in service delivery, and the ability to access information anytime, anywhere.

Section Two: Objectives of Digital Transformation

Improving Institutional Performance

Digital transformation contributes to raising the efficiency of performance within institutions through the use of modern systems and technologies that help organize work and improve the decision-making process.

•Accelerating Services

¹ Mohammed Abdel Hamid, "Cybersecurity and the Challenges of the Digital Age," Journal of Administrative Sciences, Vol. 8, No. 2 (2022): p. 55.

² Abdelkader Zerrouki, Digital Transformation in Modern Institutions, (Algeria: Dar Houma, 2023), p. 97.

³ Ahmed bin Nasser, Electronic Administration and Smart Government, (Beirut: Dar Al Nahda Al Arabiya, 2020), p. 121..

⁴ Hassan Ali, "Cyber Attacks and Protection Mechanisms," Journal of Security Studies, Vol. 6, No. 1 (2023): p. 34.

⁵ Mohamed Shawky, Network and Information Security, (Cairo: Dar Al-Jami'a Al-Jadeeda, 2021), p. 102.

⁶ Ali Mahmoud, Cybersecurity and Cyber Attacks, (Amman: Dar Safaa, 2022), p. 141.

⁷ Said Ben Khadda, Data Protection in the Digital Environment, (Algeria: Dar Al-Wa'i, 2021), p. 58.

⁸ Mohammed Al-Hadi Al-Husseini, Electronic Administration and the Challenges of Digital Transformation, 67.

⁹ Nasser Dadi Addoun, Public Administration and Modern Transformations, p. 182.

Digital transformation accelerates the completion of electronic transactions and services, saving time and effort and increasing the efficiency of administrative and service performance.

•Reducing Costs

Digital transformation helps reduce operational costs by decreasing reliance on paper transactions, simplifying administrative procedures, and utilizing digital solutions.

•Improving Service Quality

Digital transformation contributes to providing more accurate, flexible, and efficient services, thereby achieving customer satisfaction and enhancing the quality of institutional performance.

Section Three: Areas of Digital Transformation

•E-Government

E-government involves using digital technologies and information systems to manage administrative tasks and provide services, with the aim of improving efficiency and accelerating procedures within institutions.

•Digital Education

Digital education relies on the use of modern tools and technologies in the educational process, such as electronic platforms and distance learning, which contributes to facilitating access to knowledge and improving the quality of education.

•E-commerce

E-commerce refers to the buying, selling, and exchange of goods and services online, which has contributed to expanding markets and facilitating commercial transactions. Digital Health

Digital health involves utilizing modern technology to deliver healthcare services, such as electronic medical records and telemedicine consultations, with the aim of improving the quality of healthcare.

E-Government

E-government relies on the use of digital technology to provide government services to citizens and institutions, contributing to improved administrative performance, enhanced transparency, and faster transaction processing.

Section Two: The Role of Cybersecurity in the Success of Digital Transformation

Cybersecurity has become a fundamental element in the success of digital transformation projects, given its role in protecting systems, data, and electronic services from various cyber threats. With the increasing reliance on digital technology, the need for a secure digital environment that ensures service continuity and enhances user trust has grown. Therefore, this section addresses the role of cybersecurity in supporting digital transformation and the most significant challenges it faces in the modern digital environment.

First Requirement: The Importance of Cybersecurity in the Digital Environment

The importance of cybersecurity has increased with the significant expansion in the use of digital technology and the reliance of institutions on electronic systems in their various activities. Providing protection for data, networks, and digital services has become essential to ensure the safety of the digital environment and its continued efficient and secure operation.

Section One: Protecting Digital Infrastructure

• Network Protection

Cybersecurity aims to protect networks from breaches and cyberattacks through the use of protection and monitoring systems that ensure the integrity of communication and information exchange.¹

• Server Protection

Servers are among the most important components of digital infrastructure. Therefore, cybersecurity works to protect them against hacking or disruption attempts to maintain the continuity of electronic services².

Database Security

Cybersecurity contributes to protecting databases from theft, manipulation, or data loss through encryption technologies, access control systems, and backups.

Section Two: Data and Information Protection

• Data Security:

Data security aims to protect digital information from unauthorized access, modification, or destruction by adopting security methods and technologies that ensure data integrity and confidentiality.

• Digital Privacy

Digital privacy involves protecting users' personal information and preventing its exploitation or unauthorized dissemination, thus ensuring the preservation of individuals' rights within the digital environment³.

• Backup and Encryption

Backup helps preserve a copy of data for recovery in case of malfunctions or cyberattacks, while encryption protects information by converting it into unreadable

¹ Ali Mahmoud, *Cybersecurity and Cyber Attacks*, p. 150.

² Sami Abdul Karim, *Digital Security and Information Protection*, p. 84.

³ Ahmed Jamal, "Digital Privacy and User Protection", *Digital Law Journal*, Vol. 4, No. 1 (2022): p. 44.

Section Three: Enhancing Digital Trust Trust in Electronic Services

Cybersecurity contributes to enhancing the trust of individuals and institutions in electronic services by providing protection for transactions and data and ensuring the integrity of digital systems.

User Protection

Cybersecurity protects users from various cyber threats, such as hacking, information theft, and digital fraud, ensuring the safe use of digital technologies¹.

Reducing Digital Risks

Cybersecurity helps reduce cyber risks and threats by implementing preventative measures and modern technologies that decrease the likelihood of cyberattacks and their impact. The second requirement: Cybersecurity challenges in light of digital transformation

Trust in electronic services

Cybersecurity contributes to enhancing the trust of individuals and institutions in electronic services by providing protection for transactions and data and ensuring the integrity of digital systems.

Section 1: Technical Challenges

Evolving Cyber Attacks

Cyberattacks are constantly evolving in terms of methods and techniques, making them more difficult to detect and counter, and posing a significant threat to digital systems and organizations².

Weak Technical Systems

Some organizations suffer from weak technical infrastructure and information systems, making them more vulnerable to breaches and cyberattacks.

Lack of Security Updates

Failure to update systems and software regularly leads to security vulnerabilities that can be exploited by hackers, threatening data integrity and the continuity of digital services³.

Section 2: Human Challenges

Lack of Specialized Expertise

Many organizations suffer from a shortage of expertise and specialized personnel in the field of cybersecurity, which affects their ability to effectively counter cyber threats and attacks. • Weak Digital Awareness

One of the most significant challenges facing cybersecurity is the lack of digital awareness among users. A lack of knowledge about protection methods increases the likelihood of falling victim to cyberattacks and fraud.

•Human Error

Human errors, such as using weak passwords or clicking on suspicious links, contribute to security breaches that compromise the integrity of digital systems and data.

Section Three: Legal and Regulatory Challenges

Lack of Legislation

The absence of laws and regulations governing the digital space makes it difficult to combat cybercrime and protect data and information within the digital environment.

Weak Oversight

Weak oversight and security monitoring contribute to an increased likelihood of cyberattacks and breaches, impacting system security and the stability of digital services.

Transnational Cybercrime

Transnational cybercrime is among the most prominent challenges facing cybersecurity, given the difficulty of tracking perpetrators and the differences in legal frameworks between countries.

Section Three: Mechanisms for Enhancing Cybersecurity to Ensure the Success of Digital Transformation

The success of digital transformation requires a secure digital environment capable of protecting systems and data from various cyber threats. This makes enhancing cybersecurity a fundamental necessity for modern institutions. To achieve this, a range of modern mechanisms and strategies are employed, aimed at managing digital risks, developing protection methods, and raising the level of security awareness and training.

First Requirement: Modern Cybersecurity Strategies

With the continuous development of technology and the increasing number of cyber threats, it has become essential to adopt modern cybersecurity strategies to address digital risks and protect information systems. These strategies include a range of methods and techniques aimed at enhancing digital protection and ensuring the efficient and secure continuity of electronic services.

¹ Mohammed Abdel Hamid, "Cybersecurity and the Challenges of the Digital Age", p 61.

² Mohammed Al-Saleh Bouazza, Protecting Information Systems from Cybercrimes, Dar Houma for Printing and Publishing, Algeria, 2021, p. 181..

³ Ahmed Maher, Cyber Risk Management in Digital Institutions, Dar Al-Jami'a Al-Jadeeda, Egypt, 2020, p. 193.

Section One: Cyber Governance

•The Concept of Digital Governance

Digital governance refers to the set of rules, policies, and procedures that aim to regulate the use of digital technology within organizations, ensuring efficiency, transparency, and the protection of information and digital systems.¹

•Cyber Risk Management

Cyber risk management involves identifying and analyzing cyber threats and risks that may face digital systems, and implementing appropriate measures to mitigate their impact and protect data and services².

•Security Planning

Security planning refers to developing preventative plans and strategies aimed at enhancing cybersecurity by identifying protection methods, responding to incidents, and ensuring business continuity in the digital environment³.

Section Two: Modern Technologies in Cybersecurity

• Artificial Intelligence

Artificial intelligence contributes to enhancing cybersecurity by analyzing data and detecting cyber threats and attacks quickly and accurately, thus helping to improve responses to digital risks.

• Secure Cloud Computing

Secure cloud computing involves using protection technologies and procedures that ensure the security of data and information stored across cloud services, while providing confidentiality and information integrity.

• Intrusion Detection Systems

Intrusion detection systems monitor networks and digital systems to detect any intrusion attempts or abnormal activity, helping to counter cyberattacks and minimize their damage.

Third Branch: Cyber Risk Management

Risk Assessment

Risk assessment involves identifying and analyzing potential cyber threats that could affect digital systems and data, with the aim of taking appropriate measures to mitigate their impact⁴.

• Incident Response

Incident response refers to the set of actions and measures taken when a cyberattack or breach occurs, with the goal of containing the damage and restoring systems and services quickly.

• Emergency Plans

Emergency plans involve preparing proactive plans to address crises and cyberattacks, ensuring business continuity, data protection, and minimizing potential losses

Second Requirement : Cybersecurity Success Requirements

Achieving effective cybersecurity requires a set of fundamental requirements that contribute to protecting digital systems and data and ensuring the continuity of electronic services. These requirements include human resource development, legislative development, and enhanced cooperation and coordination to address various cyber threats in the modern digital environment⁵.

First Section: Formation and Training

•Human Resource Development

Human resource development is one of the most important requirements for successful cybersecurity, as it contributes to preparing qualified personnel who possess the necessary skills and knowledge to confront cyber threats and attacks⁶.

•Spreading Digital Awareness

Spreading digital awareness helps raise awareness among individuals and institutions about the importance of cybersecurity and safe methods of using technology, thus contributing to reducing digital risks.

•Continuous Training

Continuous training is a fundamental means of developing competencies and keeping pace with technological advancements and modern cyber threats, ensuring a higher level of protection and digital security.

Section Two: Legislative Development

• Data Protection Laws

¹ Ahmed Maher, Cybersecurity Risk Management in Digital Institutions, Dar Al-Jami'a Al-Jadeeda, Egypt, 2020, p. 174.

² Abdelkader Ben Azzouz, Cybersecurity and Digital Transformation in Economic Institutions, Dar Al-Khaldounia for Publishing and Distribution, Algeria, 2022, p. 189.

³ Mohamed Saleh Bouazza, Protecting Information Systems from Cybercrimes, Dar Houma for Printing and Publishing, Algeria, 2021, p. 167.

⁴ Ahmed Maher, Cyber Risk Management in Digital Institutions, Dar Al-Jami'a Al-Jadeeda, Egypt, 2020, p. 174.

⁵ Abdelkader Ben Azzouz, Cybersecurity and Digital Transformation in Economic Institutions, Dar Al Khaldounia for Publishing and Distribution, Algeria, 2022, p. 171.

⁶ Mohammed Al-Saleh Bouazza, Protecting Information Systems from Cybercrimes, Dar Houma for Printing and Publishing, Algeria, 2021, p. 145.

Data protection laws aim to ensure the security of personal information and preserve individual privacy by regulating the methods of data collection, processing, and use within the digital environment.

- **Criminalizing Cybercrimes**

Legal legislation seeks to criminalize various cyber acts and crimes, such as hacking, data theft, and digital fraud, with the goal of protecting information systems and deterring cybercriminals.

Legal Regulation of Digital Transactions

The legal regulation of digital transactions establishes a legal framework governing the use of electronic means in digital transactions and services, ensuring the protection of rights and enhancing trust in the digital environment.

Section Three: International Cooperation

Exchange of Expertise

The exchange of expertise between countries and institutions contributes to developing cybersecurity methods and leveraging successful experiences to counter cyber threats and attacks.

International Security Cooperation

International security cooperation is one of the most important means of combating cybercrime through coordination and information exchange between countries and relevant agencies to strengthen digital security.

International Agreements

International agreements establish common legal and regulatory frameworks to address cybercrime and enhance cooperation between countries in the field of cybersecurity and the protection of digital space.

Section Four: Applied Study

After addressing the theoretical aspects related to cybersecurity and digital transformation, this applied study aims to connect theory with practice by analyzing the current state of cybersecurity and its role in supporting digital transformation within institutions. This study highlights the most important challenges and practical outcomes related to cybersecurity, while offering a set of proposals and recommendations to enhance digital security and ensure the success of digital transformation¹.

First Requirement: Studying the Reality of Cybersecurity in Algerian Institutions

The cybersecurity sector in Algeria is witnessing remarkable development in light of the increasing use of digital technology within governmental and private institutions, where information systems have become an essential part of business operations and service delivery.

However, this digital transformation has been accompanied by a rise in the volume of cyber threats and attacks targeting data and digital infrastructure, making cybersecurity an imperative for protecting institutions and ensuring business continuity.

Algeria is striving to strengthen its cybersecurity framework by developing legal legislation and establishing specialized bodies for protecting information systems, in addition to adopting national strategies aimed at securing the digital space and combating cybercrime. Despite these efforts, many institutions still face challenges related to weak digital infrastructure, a shortage of qualified personnel, and a lack of awareness of the importance of cybersecurity, which affects the level of digital readiness within Algerian institutions.

Second Requirement: Analysis of the Digital Transformation Strategy in Algeria

In recent years, Algeria has been working to adopt a national digital transformation strategy aimed at modernizing public administration, improving e-services, and strengthening the digital economy. This is being achieved through the integration of modern technology in various sectors, such as education, health, administration, finance, and communications.

Algeria's digital transformation strategy is based on developing technological infrastructure, expanding internet services, encouraging the use of digital platforms, and digitizing administrative transactions and simplifying government procedures. The state also seeks to promote digital innovation and encourage investment in the technology sector and startups.

Despite these efforts, the digital transformation process in Algeria faces several challenges, including weak digital coverage in some areas, a shortage of qualified human resources, limited digital awareness, and weak cybersecurity systems. This necessitates increased investment in cybersecurity to ensure the success of digitization projects and achieve a secure digital environment.

Case Study of a Digital Organization Subjected to a Cyberattack

Many digital organizations worldwide have been subjected to cyberattacks resulting in significant material and reputational losses. Attackers typically aim to steal data, disrupt electronic services, or extort money from organizations. These attacks often involve the use of malware, distributed denial-of-service (DDoS) attacks, or phishing to infiltrate digital systems².

¹ Abdul Razzaq Bin Habib, "The Role of Cybersecurity in Protecting Digital Institutions", Journal of Security and Strategic Studies, Volume 5, Issue 2, 2023, p. 55.

² Hachichi: Cybercrimes pose a real threat to Sonatrach, Ultra Algeria, published on October 8, 2024, available at: Ultra Algeria, accessed May 22, 2026.

When an organization is subjected to a cyberattack, business continuity is affected, and user confidence in digital services declines, especially if the attack results in the leakage of sensitive data or the disruption of electronic services. The success of these attacks is often attributed to weak security measures, a lack of security updates, or human error within the organization. Countering these attacks requires adopting effective response plans that include isolating infected systems, recovering data, analyzing the causes of the breach, in addition to strengthening protection systems and security awareness to avoid the recurrence of incidents in the future.

Sonatrach is the largest national company in Algeria and one of the most important energy companies in Africa, representing the backbone of the Algerian economy through its activities in the exploitation, transportation, and export of oil and natural gas. With the expansion of digital transformation and the adoption of modern information systems, the company faces increasing challenges related to cybersecurity and protecting its digital infrastructure from cyberattacks¹. In recent years, the company's management has emphasized that cybercrime has become a real threat to the security and continuity of energy industrial facilities².

Assessing Organizational Readiness for Secure Digital Transformation:

Successful digital transformation requires a set of essential elements that ensure organizations are ready to adopt digital technology securely and effectively. This readiness includes a robust digital infrastructure, modern information systems, qualified human resources, and effective security policies to protect data and digital systems.

Cybersecurity is a pivotal element in assessing an organization's readiness for digital transformation, as the absence of cyber protection can lead to systems being vulnerable to breaches and cyberattacks, threatening the continuity of digital services and impacting the efficiency of organizational performance. The success of a secure digital transformation also depends on the extent to which organizations commit to implementing cybersecurity standards, regularly updating systems, adopting backup and encryption mechanisms, and raising digital awareness among employees and users. Therefore, achieving a secure digital transformation requires the integration of technical, human, and organizational aspects to ensure the protection of the digital environment and enhance trust in electronic services.

Conclusion:

In light of rapid technological development and the increasing reliance on digital systems, cybersecurity has become one of the most fundamental pillars for ensuring the success of digital transformation within organizations. The expansion of digital technology has contributed to improved performance and service development, but it has also led to the emergence of numerous cyber risks and threats targeting data and electronic systems.

The study demonstrated a complementary relationship between cybersecurity and digital transformation, as the success of digitization projects is linked to the ability of organizations to provide the necessary protection for digital systems and information. It also showed that adopting effective security policies contributes to enhancing trust in electronic services, ensuring business continuity, and reducing digital risks.

• Presentation of Findings

The study demonstrated that cybersecurity is a fundamental element in the success of digital transformation projects, contributing to the protection of data and digital systems from various cyber threats and attacks. It also showed that organizations adopting effective security policies are better able to ensure the continuity of their digital services and achieve higher performance efficiency.

The study further proved that the increasing reliance on digital technology is accompanied by a rise in cyber risks, necessitating the continuous development of protection mechanisms and system updates. The results also revealed a range of challenges facing organizations, including a shortage of specialized expertise, weak digital awareness, and the absence of some legislation regulating cyberspace.

• Analysis of the Relationship Between Cybersecurity and the Success of Digital Transformation

There is a close, complementary relationship between cybersecurity and digital transformation. Successful digital transformation cannot be achieved without providing a secure digital environment that ensures the protection of information and electronic systems. The higher the level of cybersecurity within an organization, the greater the users' trust in digital services, and the better the performance efficiency and service continuity.

Cybersecurity also contributes to reducing the risks associated with using digital technology, such as cyberattacks and data theft, which supports the stability of digital organizations and enhances their ability to achieve digital transformation goals. Conversely, weak cybersecurity leads to system disruptions, data loss, and a decline in trust in electronic services, hindering the success of digitization projects.

Hypothesis Testing

Through theoretical analysis and applied research, the proposed hypotheses were confirmed. It was shown that cybersecurity effectively contributes to supporting the success of digital transformation and protecting systems and data

¹ Sonatrach: Energy facilities are protected by the latest security measures, Al-Mawqi news website, available at: Al-Mawqi, accessed on: May 22, 2026.

² Mohammed Al-Saleh Bouazza, Protecting Information Systems from Cybercrimes, Dar Houma for Printing and Publishing, Algeria, 2021, p. 87.

from cyber threats. The study also demonstrated that a high level of cybersecurity leads to improved efficiency of digital services and enhanced trust in the electronic environment, while weak cybersecurity negatively impacts the stability of digital systems and hinders digital transformation projects.

Key Conclusions

- There is a complementary relationship between cybersecurity and digital transformation, as the success of the digital environment depends heavily on providing the necessary protection for electronic systems, data, and information.
- The success of digitization is linked to the effectiveness of the security policies adopted within organizations. Effective security measures contribute to enhancing trust in digital services, ensuring business continuity, and reducing cyber risks.

Future Research Prospects
This study opens the door to numerous future research areas related to cybersecurity and digital transformation, especially given the rapid development of digital technology and the increasing reliance on intelligent systems across various fields. Among the most prominent future research prospects are the following:

- **Studying the Role of Artificial Intelligence in Cybersecurity**

Artificial intelligence has become one of the most important modern technologies used in cybersecurity, contributing to data analysis and the rapid and accurate detection of cyber threats and attacks. Future research could expand to explore how artificial intelligence and machine learning technologies can be employed to predict cyberattacks and develop intelligent systems capable of automatically responding to digital risks and mitigating their resulting damage. The challenges associated with using artificial intelligence, such as sophisticated attacks and the ethical risks associated with automated systems, could also be investigated.

- **The Future of Cybersecurity in the Context of the Fourth Industrial Revolution**

The Fourth Industrial Revolution has ushered in a new digital reality based on advanced technologies such as the Internet of Things, cloud computing, robotics, big data, and intelligent systems, leading to the emergence of more complex cybersecurity challenges. Therefore, future research will explore the impact of these technological shifts on information security and digital systems, analyze the ability of institutions and countries to confront new cyber threats, and examine modern strategies that can be adopted to enhance digital protection in the context of the Fourth Industrial Revolution.

- **Cybersecurity and Smart Government**

Smart governments are increasingly reliant on digital technology to provide administrative services to citizens, making cybersecurity a fundamental element for ensuring the effectiveness and continuity of these services. Future research will examine the role of cybersecurity in protecting the infrastructure of smart governments and securing data and electronic transactions, as well as analyze the challenges governments face in protecting digital systems from breaches and cyberattacks. It will also address the extent to which digital legislation and policies contribute to enhancing trust in e-government services and achieving a secure digital transformation.

Recommendations

- **Enhancing Investment in Cybersecurity**

Enhancing investment in cybersecurity is one of the most important means of ensuring the protection of digital systems and data. This can be achieved through developing security infrastructure, adopting modern technologies, and providing the necessary resources to counter cyber threats and attacks.

• **Developing Digital Legislation**
The success of digital transformation requires the enactment of modern legislation and laws that regulate the use of digital technology and protect data and information, in addition to criminalizing cybercrimes and strengthening legal oversight within the digital space.

- **Raising the Level of Digital Training and Awareness**

Continuous training and the dissemination of digital awareness contribute to strengthening the cybersecurity culture among individuals and institutions by training users in digital protection methods and safe handling of modern technologies, thus reducing risks and human error.