Data Management as a Critical Component of Protecting Corporate Devices

Agassi Melikov[1], Vagif Gasimov[2], Samur Ahmadov[3*]

[1]*Baku Engineering University, AZ0101, 120 Hasan Aliyev Str., Khirdalan, Azerbaijan*

[2,3]*Azerbaijan Technical University, AZ1073, 25 Huseyn Cavid Ave., Baku, Azerbaijan*

(Received: June 21, 2024; Revised: June 26, 2024; Accepted: July 17, 2024; Available online: August 10, 2024)

Abstract

The relevance of the problem under study lies in the growing threat of cyberattacks and unauthorized access to corporate data. The need for effective data management at the moment is due to the increased importance of securing corporate devices, which requires in-depth analysis and understanding of the role of data management in this context. The aim of the study is to comprehensively analyze the role of information governance in securing organizational technology. The used methods were: experiment, systematization, comparison, analysis, synthesis. The main findings of the study emphasize the importance of information management in securing enterprise technology. The study involves the development of a C++ program designed to simulate different scenarios of using data management strategies. This program is designed to demonstrate the effectiveness of different information security techniques in organizational technologies. In addition, a comparative analysis of data control techniques designed to protect organizational devices has been carried out. The results of this analysis are presented in the form of a table that discusses the various aspects of information management in this context. And the developed structural diagram of information management in organizations presents the main components and processes required to secure organizational technology. The paper also provides examples of practical applications of data control techniques in large corporations, emphasizing their importance in protecting sensitive information. This research makes a practical contribution by providing organizations not only with theoretical foundations but also with concrete data governance strategies to enhance the security of corporate devices, which is essential for today's companies in the face of growing cyber threats. Limitations of the study include biases, simulated situations, and an inability to adequately address issues that arise in the actual world, such as organizational culture and cyber threats.

Keywords: Information Control, Cybersecurity of Technology Assets, Information Governance, Commercial Equipment Security, Information Security Integration

1. Introduction

The study of information governance in device security is crucial due to the increasing threat of cyber-attacks and unauthorized access to corporate data. The dramatic increase in breaches underscores the need for deeper investigation into effective data governance in securing corporate devices, as data becomes a key asset for companies. The research highlights the urgent need for effective data governance due to the increasing threat of cyber-attacks and unauthorized access to corporate information resources. Effective data governance is a strategic framework that manages, protects, and utilizes data within an organization, aiming to protect data from unauthorized access, maintain legal compliance, and ensure reliability for informed decision-making and operational efficiency. Challenges include designing and implementing strategies to ensure security, integrity, and availability of information.

For an in-depth study of this topic, previous research in this area should be analyzed. R. Balayev and F. Imanzada's [1] study emphasizes the significance of a business process improvement program in enhancing an enterprise's performance. They analyze various optimization approaches, identify contradictions, and consider modern process management methods. The authors suggest addressing errors promptly and analyzing complex management problems for improvement. Y. Imamverdiyev [2] considered the potential risks to individual data generated by Big Data technologies and highlighted the need to improve legislation in the field of protection of personal information from these threats.

Two important data protection legislation are the General Data Protection Regulation (GDPR) [3] and the California Consumer Privacy Act (CCPA) [4]. GDPR requires user consent procedures, strong security measures, and

***Corresponding author: Samur Ahmadov (samm.ahmadov@gmail.com)**

DOI: https://doi.org/10.47738/jads.v5i3.283

transparency in data collection and processing. Similar rights to GDPR, such as access, deletion, and opt-out of data sales, are granted to consumers under the CCPA. Organizations must adopt data governance procedures in order to comply with the CCPA. These procedures include keeping records up to date, updating privacy policies, and guaranteeing strong security measures. The Health Insurance Portability and Accountability Act [5] mandates that organizations perform risk assessments, set up access restrictions, use encryption, and set up audit measures in order to secure sensitive patient information in the healthcare sector. Organizations now prioritize data protection and make significant investments in strong data governance frameworks as a result of these obligations.

The article analyses current technological approaches to ensuring the security of individual information in the context of Big Data and provides an overview of current research directions. Researcher V. Qardaşov [6] focused on the efficiency of management and cost reduction in logistics companies, revealing that insufficient planning and cost control lead to serious problems in the organization of logistics processes. His recommendations derived from the study have practical applications and can have a significant impact on improving data management in companies, especially in the context of optimizing logistics activities. In turn, F.F. Yusifov and A.C. Farajova [7] discussed the world experience in the field of personal information protection in e-government, including the Estonian “Data Embassy” concept. This concept ensures the continuation of local government information centers in the face of various crises. However, despite the effectiveness of this concept, some data security issues prevent certain information from being hosted on personal clouds.

A. Abbasov and N. Karimli [8] emphasized that with the growth of internet usage and the provision of online services by companies, the threat of phishing attacks through internet domains increases. Such attacks provide new methods to obtain personal data and are also becoming more prevalent. The research focuses on the effectiveness of machine learning algorithms in detecting and preventing attacks, particularly in the context of protecting corporate network resources. The research of G.M. Aliyev [9] focuses on the security and efficiency of data transmission, but in the context of clustered wireless sensor networks. The paper proposes two methods within the same framework: for user verification and a two-level key for controlling and encrypting information. Using these methods, the security, and efficiency of enterprise devices can be optimized.

Previous studies highlight important aspects such as improving business processes to increase the efficiency of companies’ operations, identifying and minimizing risks associated with processing and analyzing large amounts of data, optimizing costs in logistics to improve business competitiveness and sustainability, ensuring strong protection of personal information when it is processed electronically, and improving the effectiveness of machine learning algorithms to prevent cyber-attacks and detect security threats. This study, however, focuses on analyzing data management as a key element in securing technological tools, which is the objective of this project.

In order to achieve the research objective, certain tasks should be highlighted. Firstly, an extensive analysis of previous research in the field can be conducted, with a main focus on the use of machine learning techniques to prevent cyber-attacks. This analysis will identify key aspects and areas of development in this field and provide a basis for further research. Secondly, it is necessary to identify and analyze the main challenges and trends in data security, focusing on the specific needs of enterprise devices. This will identify the main issues of concern and requirements for effective information management strategies in this context. And thirdly, it is required to develop and propose a methodology to evaluate the effectiveness of different data management strategies, including analyzing the application of approaches such as access control and activity monitoring. This will allow evaluating the effectiveness of the proposed strategies and identifying their advantages and disadvantages. Thus, this paper aims to further investigate enterprise device security issues and provide practical recommendations for the design and implementation of effective data management strategies.

2. Materials and Method

The methods used in this study were experiment, systematization, comparison, analysis, and synthesis. The method of experimentation was used to implement a C++ Program to simulate scenarios of information management strategies use. The experimental data obtained from the Program implementation allowed the effectiveness of different data management strategies to be evaluated in the context of enterprise technology security. Experimentation, while providing controlled environments for testing hypotheses and strategies, may have limitations due to external validity, potential biases, and the reliance on a C++ program for data management, potentially leading to oversimplified conclusions (figure 1).

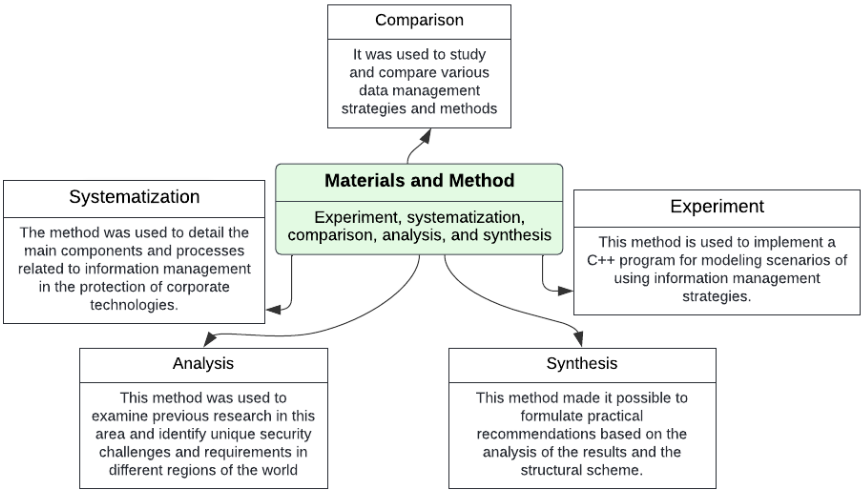

Comparison
It was used to study and compare various data management strategies and methods
Systematization
The method was used to detail the main components and processes related to information management in the protection of corporate technologies.
Materials and Method
Experiment, systematization, comparison, analysis, and synthesis
Experiment
This method is used to implement a C++ program for modeling scenarios of using information management strategies.
Analysis
This method was used to examine previous research in this area and identify unique security challenges and requirements in different regions of the world
Synthesis
This method made it possible to formulate practical recommendations based on the analysis of the results and the structural scheme.

Figure 1. Demonstration of methods and materials

This Program was written in the online integrated development environment Replit, which provides the ability to write, test and run code in different programming languages. And the resulting data allowed drawing conclusions about which data management approaches are most effective in securing enterprise technology. The systematization method was used to detail the main components and processes associated with information management in securing enterprise technology. This method allowed the information to be systematized, key aspects to be highlighted and presented in a structured manner for a deeper understanding of the research topic. The systematic description of each component and process made it possible to consider their interrelationship and importance in the context of securing organizational devices. This approach to analyzing the information management framework helped to present the main elements of their interaction and formed the basis for further analysis and discussion. Systematization can introduce biases and prioritize certain data points, potentially overlooking important aspects or alternative classifications, and leading to an incomplete or skewed representation of information governance and device security.

Through comparative analysis, different data management strategies and techniques used in different types of organizational devices were examined and compared. This approach identified similarities and differences in the data management measures used in the context of securing organizational systems. The analysis of the comparative table provided an opportunity to evaluate the effectiveness of the different approaches and highlight the most effective data management strategies for securing enterprise technologies. The analysis method was used to examine previous research in the field and to identify the unique security challenges and requirements in different regions of the world. Comparative analysis helps identify similarities and differences in data management strategies, but its effectiveness is limited by selection of comparison criteria, which can reflect researchers' biases and contextual factors, potentially resulting in universally applicable conclusions.

The data analysis assessed the impact of various factors on data management and enterprise technology security. The analysis also revealed that previous studies have identified several key aspects in the area of data management and enterprise technology security. They highlighted the importance of business process improvement programs, the need for improved legislation in the area of personal information protection, and focused on the effectiveness of cost management in company logistics. In addition, they discussed global experience in the field of privacy protection in e-government and touched upon the security of data transmission in clustered wireless networks. The analysis method, involving data examination and interpretation, can be influenced by researchers' interpretations and frameworks, leading to selective attention to evidence and potential skewing of findings due to incomplete or biased datasets.

The synthesis method was applied to integrate the findings and create recommendations for improving information management to secure organizational devices. By synthesizing the data, it was possible to identify key aspects and develop an integrated approach to data management in the context of enterprise technology security. This method also enabled the formulation of practical recommendations based on the analysis of the results and the structural framework. And the recommendations cover various aspects of information management, including information protection, availability, and accuracy, and provide a framework for improving the security of organizational technology. Synthesis can be influenced by selection bias and oversimplification, potentially leading to generalized conclusions that may not fully capture individual studies or real-world situations.

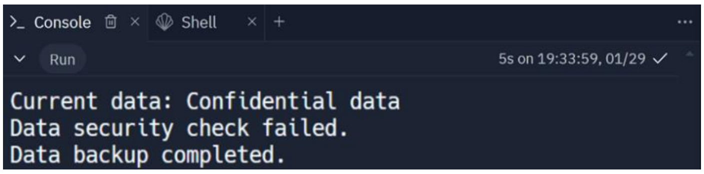
3. Results

With the introduction of modern technology solutions into the corporate environment and the inherent increase in the volume of digital information, security issues of corporate devices are becoming more acute and require fundamental consideration. Data management, as a critical component in security, is becoming a key aspect in an era where digital attacks and leaks of sensitive information are becoming increasingly sophisticated and sophisticated.

In the context of the Europe, the Middle East and Africa (EMEA) and Asia regions, enterprise device security issues are of particular relevance and complexity. EMEA is experiencing a high level of digital transformation and integration of technology into business processes. This leads to an increase in the volume of digital information, which requires reliable protection from cyber threats. Due to a variety of legal and regulatory requirements, such as the General Data Protection Regulation in the European Union, corporations in EMEA are forced to strictly comply with regulations on the processing and protection of their customers' and partners' data. Large European enterprises like Siemens and Deutsche Bank are implementing data governance strategies to comply with GDPR and other regulations, protecting customer and partner data from cyber threats. The Middle East is accelerating digital technology adoption, with companies like Saudi Aramco and Emirates Airlines integrating advanced cybersecurity measures. African countries like Kenya and Nigeria are emerging as tech hubs, requiring robust data protection measures to protect their digital assets and maintain regulatory compliance.

This emphasizes the importance of effective data governance for legal compliance and securing corporate technology. At the same time, the Asian region is experiencing rapid digitalization and a significant increase in cyber-attacks. Countries in this region such as China, India, Japan, and South Korea are emerging as leaders in information technology and digital innovation. However, this also means that they are becoming priority targets for cybercriminals and state-sponsored hacking groups. With rapid digital advances and cybersecurity threats, data governance strategies are important to protect corporate technology and sensitive information. To illustrate the role of information governance in securing organizational devices, develop a small C++ program that simulates a scenario using appropriate strategies and techniques.

First, the InformationManagement class is defined, which contains a private data field for storing information. The class constructor accepts initial data and initializes the data field. The class has three public methods: getData() – returns the current value of the data variable, simulates the retrieval of data, which is a fundamental operation in data management; updateData() – updates data with new values, simulates the modification of data, which is crucial for maintaining up-to-date information; checkSecurity() – compares the current data with a predefined security pattern to determine if the data is secure, simulates a security check mechanism, which is essential for ensuring data integrity and protection against unauthorized access. The main() function creates an instance of the InformationManagement class with the initial "Confidential data". The current information is then output, which is initialized in the constructor. Next, the data is updated to "Updated confidential data" using the updateData() method. After that, the security of the data is checked using the checkSecurity() method. In this example, it simply compares the current data to the intended security template. If the data matches the template, the message "Data is secure." is printed, otherwise the message "Data security check failed." is printed. Finally, the backupData() method is called, which outputs the message "Data backup completed.", assuming that the data was successfully copied. The completion of the data backup is indicated by the message that is produced by this procedure. It mimics the backup procedure, which is essential for data continuity and recovery in the event of breaches or data loss. The current "Confidential data" information is printed as the result. The data security check is then performed and returns true, which means that the data conforms to the security pattern. This is followed by a message that the data backup is complete (figure 2).



```
Current data: Confidential data
Data security check failed.
Data backup completed.
```

Figure 2. Result of running the program in the Replit environment

Thus, this code illustrates the basic logic of working with a class for information management and demonstrates an example of a simple data security check. A comparative analysis of information management for enterprise technology security should also be made (table 1). Enterprise devices, regardless of their type, store, and process valuable data that can be exploited by attackers. Data governance is a critical element in securing enterprise devices. It helps to protect data from various threats such as unauthorized access, data exploitation or disclosure, data corruption and data leakage.

Table 1. Benchmarking Data Control for Protecting Organizational Devices

Device	Data	Threats	Data management measures	Examples
Mobile device	Personal data of clients and employees	Unauthorized access, use, or disclosure of data	Data encryption, access control, application management	Fingerprint scanning to log in, two-factor authentication, using apps from official app stores
Server	Financial, customer and employee data	Unauthorized access, use, or disclosure of data, corruption of data	Data separation, security audit, access control	Using virtual machines to isolate data, regularly updating software, using firewalls to protect against external threats
Database	Customer personal data, financial data, and employee data	Unauthorized access, use, or disclosure of data, data leakage	Data encryption, access control, backup	Use of AES-256 encryption algorithms, restricting access to the database to authorized users only, regular data backups

Source: [10].

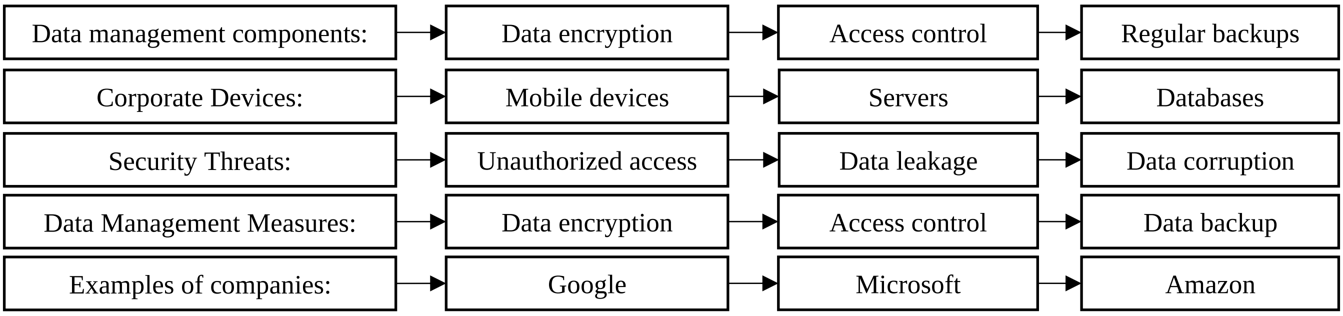
Examples of using data governance to secure enterprise devices show that applying various data governance measures can significantly improve data security. However, different types of organizational devices require different approaches to data management to ensure their security. Each type of device has different characteristics in storing and processing data, as well as vulnerabilities to possible security threats. Data management measures such as encryption, access control and backup can help protect data from unauthorized access, leakage, or corruption. And examples of the application of these measures demonstrate what practical steps can be taken to improve the security of certain devices.

It’s also important to consider how real-world corporations are applying data governance to secure their devices. For example, Google implements data encryption on mobile devices and uses data separation on servers to protect sensitive information. Google’s data governance strategy includes strict access controls, encryption, and data anonymization techniques. It uses strong protocols like TLS and AES-256 to protect data from unauthorized access. Google also implements detailed access controls and user authentication mechanisms. Continuous monitoring and auditing of data usage are also part of the strategy. Data backup is also a key practice to ensure data integrity and availability. Microsoft uses a layered security model, including encryption, access control, and advanced threat protection, two-factor authentication. Azure Active Directory manages user identities and data access, while role-based access control restricts access based on roles. Microsoft adheres to global data protection standards and provides compliance scores through its Compliance Manager tool. It also uses data analytics to identify potential security threats and anomalous activity. Amazon, on the other hand, with its focus on cloud computing, offers a variety of security tools such as data encryption and access control to ensure that information in the cloud is protected. Amazon Web Services (AWS) offers a robust data governance framework focusing on security, compliance, and operational excellence. It provides tools like AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), and AWS CloudTrail to help organizations secure and manage their data. In addition, Google uses fingerprint scanning to access mobile devices, Microsoft uses virtual machines to isolate data on servers, and Amazon uses encryption algorithms to protect data in databases. These companies demonstrate how different data management measures can be adapted and used to secure different devices and data. However, despite the differences in approaches, their goal remains the same – to protect data from security threats.

Based on the analysis, a few key recommendations can be identified. That is, organizations should proactively implement data governance measures such as encryption, access control and regular backups to ensure the security of their technology systems. This will help protect data from various threats such as unauthorized access, leaks, or corruption. Additionally, it's critical to modify data management strategies based on the type of device. For mobile devices, biometric-based authentication techniques can be used and for servers – data separation and virtualization techniques. Furthermore, it is important to provide personnel with training on data security and management methodologies in order to mitigate human error-related security breaches and enhance organizational culture. Programs for awareness and training should include how to spot phishing attempts, comprehend the strategies used by attackers, and react correctly. Additionally, they must to advocate for data management best practices, such data categorization, safe storage, and appropriate disposal of private data. Employees should learn about their duties for ensuring data security and be encouraged to comply with data protection rules and regulations, such as GDPR, HIPAA, and CCPA, through training programs.

Regular updates to security policies and data management practices are necessary to keep up with changing threats and regulatory requirements. This will help maintain a high level of security in the long term. In turn, the use of modern technologies such as data analytics and cloud computing should also be considered. These technologies can greatly improve the effectiveness of security and data management measures. Integration strategies for integrating data analytics and cloud computing into data governance strategies include hybrid cloud solutions, data governance platforms, data encryption and access controls, continuous monitoring and auditing, and compliance management features. Hybrid cloud solutions combine on-premises and cloud-based data storage and processing, while data governance platforms provide centralized dashboards for monitoring data quality, compliance, and security. Data encryption and access controls, such as multi-factor authentication and role-based access controls, are essential for securing data in the cloud. Continuous monitoring and auditing of data access and usage are essential for maintaining data security and compliance. Cloud services with built-in compliance management features help automate compliance reporting and track regulatory changes.

Finally, organizations should continuously monitor and analyze the effectiveness of their security and data management measures to respond quickly to new threats and changes in the environment. This will help to maintain a high level of data protection and minimize the risks of security breaches. It is also worth creating a structural diagram to show the main components and processes related to information management in securing enterprise technology (figure 3).



Data management components: → Data encryption → Access control → Regular backups

Corporate Devices: → Mobile devices → Servers → Databases

Security Threats: → Unauthorized access → Data leakage → Data corruption

Data Management Measures: → Data encryption → Access control → Data backup

Examples of companies: → Google → Microsoft → Amazon

Figure 3. Information management structure in ensuring the security of corporate technologies

Figure 3 demonstrates the relationship between the main components and processes of data governance in the context of securing organizational devices. Consequently, the study analyzed the role of data governance in securing organizational technology. To do so, a variety of methods including experimentation, systematization, comparison, analysis, and synthesis were used to examine various aspects of the problem. The results of the study lead to certain key findings. Firstly, information management plays a crucial role in securing enterprise technologies. Effective data governance helps to protect valuable data from various threats such as unauthorized access, information leakage and malicious attacks. Secondly, various information management techniques such as encryption, access control, backup, and monitoring are key tools in securing organizational technology. Third, each type of organizational device requires a tailored approach to data management, taking into account its specific characteristics and potential vulnerabilities. Fourth, large corporations such as Google, Microsoft, and Amazon have demonstrated effective use of various data management practices to secure their technology systems. Fifth, it is important to ensure that security policies and data management practices are constantly updated to adapt to changing threats and regulatory requirements. Thus, this study represents an important contribution to the understanding of the role of information governance in securing organizational technology and opens new perspectives for future research in this area.

4. Discussion

To analyze this topic in more depth, it is worth exploring other research on data governance, which represents a key element in securing corporate devices. K. Najaf et al. [11], H. Wu and Y. Wang [12] emphasize the importance of corporate governance, which involves rules and mechanisms to guide companies, ensure efficient operation, and balance interests. The importance of effective governance has grown due to financial crises and financial institution expansion. To protect their data, companies have implemented corporate data governance, which is different from conventional data management. This approach assesses, guides, and protects data and related infrastructure, focusing on its value and risk identification. The importance of managing and safeguarding data in the context of the corporate environment is shared by the mentioned works and this paper, but the latter study provides a more comprehensive view by demonstrating how data itself becomes a vital asset for businesses and needs particular governance to ensure its security. Although studies by K. Najaf et al. and H. Wu and Y. Wang are insightful, they might not be technical or flexible enough to handle risks to data security. The focus on conventional corporate governance practices, such as committees and internal controls, could not fully address the dynamic nature of data security issues, which might impede the pace at which new threats and technical breakthroughs are adapted.

Works by M. Farooq et al. [13], T. Odintsova [14] aimed to develop algorithms for protecting IoT devices using various firewalls and evaluate their effectiveness. The results showed that firewalls, configured to filter traffic and monitor IoT communications, achieved 99% accuracy in protecting devices from cyber threats, confirming the effectiveness of firewall algorithms for IoT security. The studies offer a thorough technical focus on a particular subset of organizational technology, which enhances the present research. Beyond IoT security, the current study provides a more comprehensive perspective by including a range of organizational device types and general data governance procedures. Although M. Farooq's work is very technical and thorough, it might be improved by addressing more extensive governance frameworks and rules, which are crucial for effective data governance. The findings of the research by T. Odintsova can help with defense strategy development and comprehension of the dangers and vulnerabilities related to IoT devices. But, it's crucial to take into account the security of other kinds of devices when developing a complete cybersecurity plan, as a breach in any one of them might endanger the system as a whole.

M. Yusuf et al. [15] and V. Kamala et al. [16] conducted studies on the impact of information technology development management and blockchain adoption on corporate governance. The studies found that effective corporate governance is crucial for mitigating risks and protecting investors' interests. The potential of technological innovation to improve IT governance and corporate governance within the blockchain framework is also noted. Their studies highlight the importance of good corporate governance to reduce risks and protect investors' interests. Given the quick advancement of IoT technology and the rise in internet-connected devices, the findings of these research may prove helpful in formulating security protocols for smart devices. However, the current study presents a larger range of technical views, including cloud computing and data analytics and how they are employed in data governance, whereas they only address certain parts of technology's influence on corporate governance. One disadvantage of the M. Yusuf et al. study is that it may have ignored other complementary technologies that might enhance data governance protocols in favor of blockchain technology. The work on smart device security by V. Kamala et al. is important, particularly in light of developments in the Internet of Things, but the incorporation of blockchain technology has to be carefully studied.

The study by H. M. Naguib et al. [17] explores the impact of IT and data management on IT performance in the telecoms sector. A survey of 308 managers found that IT and data management significantly affect financial and non-financial performance, with IT governance having a greater impact on financial performance and data governance on business processes and ethical compliance. As a result, data governance is the main emphasis of both initiatives, with the aforementioned research being unique in that it also takes performance-related IT governance into account. It attests to the important influence data management has on business productivity. But other aspects, such as market shifts and technological progress, also need to be taken into account. While the latter study focuses on the realistic implementation of data governance procedures through simulation, H. M. Naguib et al.'s research offers more empirical evidence relating governance approaches to performance results. The level of technical implementation in H. M. Naguib et al.'s work may have been restricted, which is something that the present research addresses more thoroughly.

A. Sadiqui [18] explored network traffic, device security, control, and data plane. The control plane includes traffic between devices for network configuration. The paper discusses connection restrictions, administrative roles, and access protection using privilege levels. It also covers configuration file and system security, automated security features, and control plane security. Privilege levels define a user’s ability to execute certain commands on a router, and Cisco devices typically have three default privilege levels: zero, user, and privileged. The main focus of the study is network device security, with a particular emphasis on network segmentation, firewall configuration, and access restrictions. A. Sadiqui concentrates on network-specific security measures, in contrast to the latter research's generic approach, which takes into account a wide range of organizational devices and data governance procedures. The focused strategy is different from the more general focus of the current study on data governance across different kinds of devices. The more comprehensive data management and governance needs for various organizational devices and data kinds may not be entirely covered by A. Sadiqui's study. Technical solutions should be coupled with more comprehensive data governance frameworks to provide strong data security.

K. Mehdi’s [19] study highlights the saturated data management market, addressing challenges like data integration, security, and compliance. The goal is to shift corporate culture by putting data governance at the center of decision-making. The study outlines key functions of data management tools and 12 technology functions for developing a data-centric approach. While K. Mehdi's work emphasizes the relevance of data management in decision-making, the current research underlines information management as a fundamental component of device security. Businesses trying to enhance their device security and streamline their data management procedures may find value in the findings of the previously mentioned study. However, other factors like data integration and compliance must also be taken into account in order to completely execute a data-centric strategy in an organization. N. Xu et al. [20] emphasize that a good data governance framework aligns with corporate governance objectives to strengthen a corporation’s contribution to market integration and economic performance. Telecommunication companies view data governance as a tool to ensure data quality and protect it as a corporate asset, increasing transparency, accountability, independence, and fairness in corporate governance implementation. While N. Xu et al. link data governance to more general business goals, the present research concentrates primarily on the technical and practical elements of protecting organizational data. The 2024 study's novel methods and useful recommendations can assist achieve corporate governance more fairly, transparently, and accountably. However, each company's unique needs and those of its industry must be taken into account in order to properly execute these guidelines [21], [22].

Author S. Huang [23] highlighted that the emergence of big data has led to changes in the way organizations collect, process and analyze information. This paper discusses the key aspects of data security in cloud environments, focusing on strategies for protecting sensitive information, access control and privacy. By analyzing various studies and best practices in this area, the author aims to provide valuable guidance to organizations that want to use cloud computing for big data analytics while maintaining privacy and strict access control. Data protection and management are common aspects. However, the present research examines information in the context of safeguarding business devices, whereas the cited work concentrates on data security in cloud settings. While S. Huang results emphasize privacy, confidentiality, and strong access controls in managing large data, they also lay a special emphasis on cloud-specific difficulties that are in line with the present research's emphasis on data governance. The 2024 study's findings can be helpful to businesses that employ cloud-based data solutions because cloud environments are become more common and need strong security measures [24], [25].

A project of authors A. Kumar et al. [26] investigated the need for a modern data warehouse, which is not only in conceptual aspects but an integral component. Data queries are increasing in volume, velocity, validity and complexity, presenting increasing challenges for management and security. Data democratization and data security are at opposite poles, but the need for effective governance exists to strike a balance between the two. There are many tools and methods for this, but the essence of the concepts, processes and possible risks can be found in cloud services. The administration and preservation of data is a common theme across both studies, underscoring the significance of data in the modern information society. The democratization of data, or improved access to and use of data by various user groups, is a further topic covered by the research by A. Kumar et al. The results may be helpful to businesses dealing with the increasing difficulties in data management and security. But the emphasis on democratization can obscure technological safeguards for reliable data security, and the theoretical conversation might not adequately represent real-world difficulties [27]. It is essential to incorporate technology solutions with more general organizational procedures.

The study by S. Sultana and J. Sangeetha [28] emphasizes the importance of security in infrastructure, particularly smart home systems. The research aims to secure remotely managed home infrastructure and reduce power consumption of smart devices. The study uses a web application to control appliances, allowing authorized users to remove unused or hacked devices. Encryption is used for data storage and transmission, with a focus on authentication, verification, and energy reduction. Although the emphasis of both studies is device security, the circumstances are different in this case, the corporate environment is the home infrastructure, whereas in the other – the business environment. This highlights the necessity of using different security techniques based on the situation. Although S. Sultana and J. Sangeetha's study on smart device security in home automation systems provides insightful information, corporate data governance requirements might not be entirely addressed. Integrating technological solutions with more comprehensive data governance frameworks that address organizational and technical elements of data protection is essential to ensuring strong data security [29], [30].

P. Gupta's [31] study highlights the importance of data governance in organizations, particularly in environments with multiple users. It highlights the potential of modern technologies like artificial intelligence and machine learning in improving data governance processes, analyzing methods for enhancing management practices and exploring their limitations. The implication is that both papers look at aspects of data management and the application of modern technologies. However, in contrast to the study by P. Gupta, the current research focuses on device protection. The results of the analyzed work may be useful for companies seeking to improve their data management practices using modern technologies but it is important to keep in mind that device protection is also a critical aspect of data security, and its omission can create serious vulnerabilities in the system [32], [33].

Thus, various studies have highlighted the importance of data management and IT security in various sectors including telecommunications, cloud computing, enterprise environments and automation. Previous studies have also highlighted the potential of modern technologies such as blockchain, artificial intelligence and machine learning in improving data management processes and security. However, this study combines the topic of information management and device security, which is not present in previous works.

5. Conclusions

Research findings have confirmed that data management and information technology security play a key role in modern organizations, regardless of their industry and size. Analyses of various studies have shown that proper data management contributes to improving the efficiency of business processes and increasing the competitiveness of companies. Based on the findings, it can be concluded that in the context of digital transformation, data management is becoming a necessity for the successful functioning of any organization.

The increasing amount of data and rapid processing speed pose a threat to information security. Therefore, developing effective data protection strategies and using advanced encryption technologies are crucial for organizations. Enterprise management and IT departments should prioritize cybersecurity measures. Analysis techniques like experimentation, systematization, comparisons, and synthesis have identified the importance of effective data management in protecting sensitive information. A C++ program simulates data management scenarios and compares data control techniques, providing practical tools for improving organizational technology security. This study highlights the theoretical aspects of data governance and provides strategies to enhance enterprise device security, contributing significantly to cybersecurity.

Organizations should develop comprehensive cybersecurity and data governance plans that consider their unique business needs and risks. They should allocate resources for incident response and ongoing cyber threat investigation and implement specialized monitoring systems, protection systems, network traffic monitoring, multi-layered data protection measures, and identity and authentication systems. Collaboration with external cybersecurity service providers can enhance data security. Data governance measures like encryption, access control, and regular software upgrades should be implemented to protect technology systems from threats. Customizing data management approaches, training staff on data security, and regularly updating security policies are essential. Modern technologies like data analytics and cloud computing can enhance security and data management effectiveness. Continuous monitoring and analysis are crucial for quick response to new threats and environmental changes.

The practical significance of the study is to provide companies of any size and industry with specific recommendations, strategies to improve IT security and data management and effective measures to protect sensitive information and prevent cyber threats. Future research in this area should examine the effects of new encryption techniques, the impact of information technology developments on data security, the analysis of cybersecurity system vulnerabilities, and the influence of laws and regulations on the data management and cybersecurity strategies of organizations. It should also look into the implications of emerging technologies integration, industry-specific data governance challenges, the influence of user behavior on data security, and the changing regulatory landscape.

6. Declarations

6.1. Author Contributions

Conceptualization: A.M., V.G., and S.A.; Methodology: S.A.; Software: A.M.; Validation: A.M. and V.G.; Formal Analysis: A.M. and V.G.; Investigation: A.M.; Resources: S.A.; Data Curation: S.A.; Writing Original Draft Preparation: A.M. and V.G.; Writing Review and Editing: S.A. and A.M.; Visualization: A.M.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] R. Balayev and F. Imanzada, “Features of improving the management of business processes,” *PAHTEI: Proc. Azerbaijan High Tech. Educ. Inst.*, vol. 29, no. 6, pp. 70-79, 2023.

[2] Y. Imamverdiyev, “Big data and personal data security,” *In: 1st Repub. Sci.-Pract. Conf. “Big Data: Possibilities, Multidiscipl. Probl. Perspect.”,* vol. 2016, no. February, pp. 109-113.

[3] General Data Protection Regulation (GDPR). 2016.

[4] California Consumer Privacy Act (CCPA). 2020.

[5] Health Insurance Portability and Accountability Act (HIPAA). 1996.

[6] V. Qardaşov, “A company’s logistics costs and their management”; *Sci. Rev. Azerbaijan State Univ. Econ,* vol. 10, no. April-June, pp.105-115, 2023.

[7] F. F. Yusifov and A. C. Farajova, “Protection of personal data in electronic governance: “Data embassy” concept”, *Probl. Inf. Soc.*, vol. 2021, no. 2, pp. 119-130.

[8] A. Abbasov and N. Karimli, “Fishing method and anti-fishing methods”, *PAHTEI: Proc. Azerbaijan High Tech. Educ. Institut.*, vol. 30, no. 7, pp. 59-71, 2023.

[9] G. M. Aliyev, “Secure and effective data transfer for cluster-based wireless sensor networks”, *Sci. Work*, vol. 16, no. 4, pp. 309-316, 2022.

[10] CIS Benchmarks List, 2024.

[11] K. Najaf, A. Chin, A. L. W. Fook, M. M. Dhiaf, K. Asiaei, “Fintech and corporate governance: at times of financial crisis”, *Electron. Commer. Res*, vol. 24, no. 1, pp. 605-628, 2024.

[12] H. Wu and Y. Wang, “Digital transformation and corporate risk taking: Evidence from China”, *Global Finance J.*, vol. 62, no. September, pp. 1-20, 2024.

[13] M. Farooq, R. Khan and M. H. Khan, “Stout implementation of firewall and network segmentation for securing IoT devices”, *Indian J. Sci. Technol.*, vol. 16, no. 33, pp. 2609-2621, 2023.

[14] T. Odintsova, “Updating the Informational and Control Practices in the Sustainability Agenda”, *Econ. Cult.*, vol. 21, no. 1, pp. 133-148, 2024.

[15] M. Yusuf, L. Hakim, J. Hendra, K. Kamar, W. Idawati, E. Winarso, C. Meiden and M. Fahlevi, “Blockchain technology for corporate governance and IT governance: A financial perspective”, *Int. J. Data Network Sci.*, vol. 7, no. 2, pp. 927-932, 2023.

[16] V. Kamala, D. Arun, R. Aswin Raj, S. Gokulakrishnan and S. Harshil, “Securing smart devices on blockchain”, *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 5, pp. 5544-5549, 2023.

[17] H. M. Naguib, H. M. Kassem and A. E. H. M. A. Naem, “The impact of IT governance and data governance on financial and non-financial performance”, *Future Business J.*, vol. 10, no. 15, pp. 1-22, 2024.

[18] A. Sadiqui, “Securing network devices”, *In: Computer Network Security. London: ISTE Ltd.*, vol. 2020, no. February, pp. 15-40.

[19] K. Mehdi, “Data governance tools”, *In: Data Governance, Cham: Springer*, vol. 2023, no. December, pp. 121-137.

[20] N. Xu, W. Lv, J. Wang, “The impact of digital transformation on firm performance: a perspective from enterprise risk management”, *Eurasian Bus. Rev.*, vol. 14, no. 2, pp. 369-400, 2024.

[21] S. Kerimkhulle, Z. Dildebayeva, A. Tokhmetov, A. Amirova, J. Tussupov, U. Makhazhanova, A. Adalbek, R. Taberkhan, A. Zakirova and A. Salykbayeva, “Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things”, *Symmetry*, vol. 15, no. 10, pp. 1-29, 2023.

[22] O. Havrysh, Y. Obruch, A. Chepynoga, A. Honcharov and O. Panasko, “Organizational structure of technical protection of information at the network level using vpn technology”, *Bull. Cherkasy State Technol. Univ.*, vol. 28, no. 3, pp. 5-15, 2023.

[23] S. Huang, “Big data processing and analysis platform based on deep neural network model”, *Syst. Soft Comput.*, vol. 6, no. December, pp. 1-6, 2024.

[24] I. Opris, S.C. Ionescu, M.A. Lebedev, F. Boy, P. Lewinski and L. Ballerini, “Editorial: Application of Neural Technology to Neuro-Management and Neuro-Marketing”, *Front. Neurosci.*, vol. 14, no. 1, pp. 25-53, 2020.

[25] A.I. Leonow, M.N. Koniagina, S.V. Petrova, E.V. Grunt, S.Y. Kerimkhulle and V.G. Shubaeva, “Application of information technologies in marketing: Experience of developing countries”, *Espacios*, vol. 40, no. 38, pp. 1-10, 2019.

[26] A. Kumar, A. Mishra and S. Kumar, “Data democratization, governance, and security”. *In: Architecting Modern Data Warehouse Large Enterprises, Berkeley, CA: Apress*, vol. 2023, no. December, pp. 255-305.

[27] I. Metelskyi and M. Kravchuk, “Features of cybercrime and its prevalence in Ukraine”, *Law Policy Sec.*, vol. 1, no. 1, pp. 18-25, 2023.

[28] S. S. Sultana and J. Sangeetha, “Securing the smart devices in home automation system”, *In: Cyber Security, Privacy Networking. Singapore: Springer*, vol. 2022, no. May, pp. 273-285.

[29] N. Mentukh and O. Shevchuk, “Protection of information in electronic registers: Comparative and legal aspect”, *Law Policy Sec.*, vol. 1, no. 1, pp. 4-17, 2023.

[30] V. Malinovskyi, L. Kupershtein and V. Lukichov, “Mathematical model for assessing cyber threats and information impacts in microcontrollers”, *Inf. Technol. Comput. Eng.,* vol. 59, no. 1, pp. 69-82, 2024.

[31] P. Gupta, “The role of AI in crafting a modern data governance”, *Int. Res. J. Modernization Eng. Technol. Sci.,* vol. 6 no. 1, 266-271, 2024.

[32] L. Savytska, T. Korobeinikova, O. Kostiuk, I. Kolesnyk and O. Dudnyk, “Internet of things protection means in the corporate computer network”, *Inf. Technol. Comput. Eng.,* vol. 59, no. 1, pp. 83-93, 2024.

[33] A. Nafiiev and D. Lande, “Malware detection model based on machine learning”, *Bull. Cherkasy State Technol. Univ.,* vol. 28, no. 3, pp. 40-50, 2023.