Üçüncü Sektör Sosyal Ekonomi Dergisi
Third Sector Social Economic Review
60(3) 2025, 3334-3356
doi: 10.63556/tisej.2025.1588

Research Article

The Relationship Between Cybersecurity, Corporate Trust and Corporate Reputation in Businesses

İşletmelerde Siber Güvenlik, Kurumsal Güven ve Kurumsal İtibar Arasındaki İlişki

Polathan KÜSBECİ	**Mehmet Fatih BURAK**
Asist. Prof. Dr. Istanbul Nişantaşı University	Dr., Istanbul Beykent University
Management Information Systems	Institute of Graduate Studies
scholar@polathan.com	m.fatih@msn.com
https://orcid.org/0000-0002-4858-3853	https://orcid.org/0000-0002-9187-6491

Makale Geliş Tarihi	**Makale Kabul Tarihi**
07.07.2025	**15.09.2025**

Abstract

This study explores the relationship between cybersecurity, corporate trust, and corporate reputation an area that has received limited attention in previous research. A quantitative research design, convenience sampling method was adopted and data were collected through a structured questionnaire administered to 252 participants working in various departments of different organizations. Participants were selected using a convenience sampling method, targeting individuals who were easily accessible and willing to participate. The data were analyzed using the SPSS and AMOS programs, applying descriptive statistics, factor analyses, reliability and validity analyses, correlation, and regression analyses to examine the associations among the variables. The findings reveal that cybersecurity positively and significantly influences both corporate trust and corporate reputation. Additionally, corporate trust was found to have a positive and significant impact on corporate reputation. These results highlight the critical role of cybersecurity not only in protecting information but also in shaping stakeholders' perceptions and trust in organizations. By establishing a strong cybersecurity infrastructure, businesses can enhance their reputation and strengthen trust among employees, customers, and partners. This study contributes to the literature by empirically demonstrating these relationships and offers practical implications for organizational leaders aiming to improve their strategic positioning and long-term sustainability. It also provides a valuable foundation for future research in the fields of cybersecurity management and organizational behavior.

Keywords: *Cybersecurity, Corporate Trust, Corporate Reputation, Digitalization, Information Systems*

Öz

Bu çalışma, daha önce literatürde sınırlı şekilde ele alınmış olan siber güvenlik, kurumsal güven ve kurumsal itibar arasındaki ilişkiyi incelemektedir. Nicel bir araştırma deseni, kolayda örnekleme yöntemi benimsenmiş ve veriler, farklı kurumların çeşitli departmanlarında görev yapan 252 katılımcıya uygulanan yapılandırılmış bir anket aracılığıyla toplanmıştır. Katılımcılar, kolayca ulaşılabilen ve katılmaya istekli bireyleri hedefleyen kolayda örnekleme yöntemi kullanılarak seçilmiştir. Elde edilen veriler SPSS ve AMOS programları kullanılarak tanımlayıcı istatistikler, faktör analizleri, güvenilirlik ve geçerlilik analizleri, korelasyon ve regresyon analizleri ile değerlendirilmiştir. Bulgular, siber güvenliğin hem kurumsal güven hem de kurumsal itibar üzerinde olumlu ve anlamlı bir etkisinin olduğunu ortaya koymuştur. Ayrıca, kurumsal güvenin kurumsal itibar üzerinde pozitif ve anlamlı bir etkisi olduğu saptanmıştır. Bu sonuçlar, siber güvenliğin yalnızca bilgiyi korumada değil, aynı zamanda paydaşların algılarını ve kuruma duyduğu güveni şekillendirmede de kritik bir rol oynadığını göstermektedir. Güçlü bir siber güvenlik altyapısı oluşturarak, işletmeler itibarlarını artırabilir ve çalışanlar, müşteriler ve iş ortakları arasında güveni pekiştirebilir. Çalışma, bu ilişkileri ampirik olarak ortaya koyarak literatüre katkı sağlamakta ve stratejik konumlanmalarını ve uzun vadeli

Önerilen Atıf /Suggested Citation
Küsbeci, P. & Burak, M.F., 2025, The Relationship Between Cybersecurity, Corporate Trust and Corporate Reputation in Businesses, *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 60(3), 3334-3356.

sürdürülebilirliklerini geliştirmek isteyen yöneticilere pratik öneriler sunmaktadır. Ayrıca, siber güvenlik yönetimi ve örgütsel davranış alanlarında yapılacak gelecekteki araştırmalar için de değerli bir temel oluşturmaktadır.

Anahtar Kelimeler: *Siber Güvenlik, Kurumsal Güven, Kurumsal İtibar, Dijitalleşme, Bilişim Sistemleri*

1. Introduction

In the digital world, with every device connected, cybersecurity has become more important in terms of data and technology security. With the rapid development and change of digital transformation and the connection of many devices to each other, cybersecurity threats are becoming more complex every day. This situation reveals that cybersecurity is of vital importance for ensuring the security of individuals, organizations, and states. Cybersecurity undertakes the task of protecting from unauthorized access, malicious software, and cyberattacks. Thus, it protects computer networks, servers, information systems, data, and digital resources of individuals or organizations. Along with the developments brought by Industry 4.0, the increasing prevalence and sophistication of cyberattacks are associated with many organizations adopting new measures. This situation requires organizations to constantly take precautions not only against external threats but also against dangers coming from within. Securing the digital infrastructures of organizations is important for the performance of the organization and it is necessary to develop a solid cybersecurity strategy for possible future risks (Toussaint et al., 2024). Cybersecurity measures are both a technological and organizational necessity. If cybersecurity measures are not taken promptly, this is associated with serious damage to the reputation of organizations, loss of employee trust, and potential financial losses.

Corporate reputation, which determines how the outside world perceives an organization, is an important factor in determining the trust and loyalty of its stakeholders. The image that the institution or organization presents to the society, and the actions it carries out for its future goals from the past are important in shaping the reputation. Corporate reputation should not be considered only as the appearance it presents to the outside world. Because corporate reputation also includes the trust and loyalty of stakeholders. The survival of a company is of course related to its financial performance. Businesses that can manage their reputation well will be able to make significant progress in company performance. This helps in strengthening customer loyalty. Corporate reputation management has become a critical strategy for companies to maintain their long-term success in gaining a competitive advantage in the market and strengthening their market position. At the same time, cybersecurity has a significant impact on the reputation of the institution. A cybersecurity breach can seriously shake the reputation of the company (Hamidi et al., 2023). The work information of institutions exposed to cyber attacks may be associated with the theft of employee information. This situation is associated with potential financial losses for the institution and may also be linked to a loss of employee trust. Since the feeling of trust forms the basis of relationships with the institution, taking cybersecurity measures is also vital for the protection of corporate reputation.

Corporate trust is important in maintaining healthy relationships between individuals in an organization and in effectively maintaining cooperation. Establishing an environment of trust should not only be considered between individuals. As long as the environment of trust continues correctly between employees and managers, relationships between employees will continue more effectively and efficiently. The success of an organization is its ability to innovatively design products that can meet the demands and needs of customers. This can be achieved through the trust, communication, and motivation that employees have for each other. This environment of trust is also critical to the long-term success of employees and creates higher productivity and a stronger team spirit. The lack of organizational trust can create insecurity, uncertainty, and conflict among employees. A safe working environment not only increases employee loyalty but also increases the overall efficiency of the organization (Ramish et al., 2024).

The trust model introduced by Mayer, Davis, and Schoorman (1995) provides a comprehensive theoretical basis for examining the relationship between cybersecurity, corporate trust, and reputation. This model suggests that trust hinges on stakeholders' views of the trusted entity's competence, goodwill, and integrity. In the realm of cybersecurity, stakeholders perceive the robustness of an organization's technological systems and its proactive defense measures against cyber threats as indicators of organizational competence. Additionally, the adoption of cybersecurity practices marked by openness and responsibility strengthens perceptions of goodwill and ethical behavior, thereby nurturing a trusting environment. Such trust, recognized by both internal and external parties, plays a crucial role in bolstering corporate reputation. As a result, cybersecurity is not only a technical necessity but also a critical strategic resource for maintaining enduring corporate trust and reputation (Mayer et al., 1995). Taking the necessary precautions in terms of cybersecurity is an important factor in both protecting corporate reputation and creating trust among employees. Therefore, cybersecurity

practices stand out as strategic elements that complement each other in ensuring corporate reputation and strengthening corporate trust. Managing these three factors together in institutions is of critical importance to ensure the long-term sustainability and success of institutions.

This study aims to examine the relationship between cybersecurity, corporate trust, and corporate reputation—an area that has been relatively underexplored in the existing literature. In recent years, the growing importance of cybersecurity has attracted considerable attention across various fields, particularly in relation to organizational performance, trust, and reputation. While extensive research has been conducted on these individual concepts, studies that simultaneously explore the relationship between cybersecurity, corporate trust, and corporate reputation remain scarce. In this study, the concepts of cybersecurity, corporate trust, and corporate reputation are first introduced. Then, the methodology section is presented, followed by the results and conclusions.

2. CyberSecurity

Cybersecurity plays a critical role in ensuring the security of an organization or even a country. It requires the integration of various technologies, cultural elements, resources, and structures to maintain the security, continuity, and integrity of data in cyberspace (Hussain et al., 2020: 2). Cybersecurity is the entirety of technologies, processes, and methods designed, developed and implemented to protect corporate assets, customer information, and intellectual property from unauthorized access and misuse. Not only unauthorized personnel, but also other potential threats can damage sensitive data. In general, cybersecurity is a comprehensive approach organizations adopt to manage the risks of unauthorized access and authorized misuse (Kaur et al., 2021: 17-18). Cybersecurity is a discipline that ensures the integrity, confidentiality, and availability of information in complex interactions in network environments. With the developments in technology and the increasing number of devices connected daily, cybersecurity has become a critical issue for all businesses. As a result of this situation, the risk of cyber-attacks increases significantly (Durst et al., 2023: 2).

Cybersecurity issues are gaining more and more attention worldwide. This discipline aims to ensure security by protecting networks, computers, servers, and information connected to the Internet against attacks that may come from unauthorized access (Rajan et al., 2021: 2). Cybersecurity, which is of critical importance today, allows governments, companies, and financial institutions to manage sensitive information through information technology and, from time to time, transfer this data to other systems over networks. To overcome this challenge, each organization needs to identify cybersecurity risks with processes such as risk assessment tools, risk escalation, and threat detection tools to identify confidential information. After identifying risks, organizations need to evaluate their overall ability to protect and maintain their systems and devices (Al-Alawi and Al-Bassam, 2020: 1525). Organizations are trying to secure their operations by making their cybersecurity ecosystems more complex and using people, technology, and processes in an integrated way. However, cybersecurity breaches, which usually result in the theft of customer data, can impose significant financial burdens on organizations. These financial burdens; cover various items such as notification to affected persons, legal expenses, fines, and recovery efforts from the effects of the breach (Ogbanufe et al., 2021: 1). Every organization uses various technologies and tools to maintain its daily operations, while at the same time, it must constantly monitor its operations to protect these assets from various threats. Auditing the information technology environment is a fundamental component of cybersecurity auditing and requires appropriate tools, technologies, and technical knowledge. Audit controls in network and computer systems play an increasingly critical role in the operational security of organizations. However, every organization should consider various factors such as different frameworks, standards, and technologies when implementing these audits and determining audit tools and controls. Information systems (IS) auditors and cybersecurity professionals should approach an integrated audit framework with a clear vision. This framework should focus on the latest technologies and functions in the cybersecurity field, while also collaborating with the management level to determine cybersecurity audit tasks and procedures to address potential threats (Al-Matari et al., 2021: 189).

The GDPR (General Data Protection Regulation) is a comprehensive regulation of critical importance for financial institutions in terms of protecting personal data, preventing data breaches, and avoiding heavy penalties (Voigt & Von dem Bussche, 2017). PCI DSS, on the other hand, is a mandatory security standard aimed at protecting payment card information and ensuring the security of financial transactions, helping organizations reduce security vulnerabilities and increase customer trust (PCI Security Standards Council, 2018). Highlighting the importance of these regulations both for legal compliance and for safeguarding

institutional reputation will significantly enhance the depth and quality of cybersecurity analyses in the financial sector.

Organizations in various sectors are becoming more vulnerable to cybersecurity breaches in an era shaped by a rapidly changing threat environment and unique technological advances (Olaniyi et al., 2023: 128). New threats brought about by the Fourth Industrial Revolution have created an increasing need for the control and protection of information in cyberspace in terms of state security. This situation offers critical opportunities to defend against attacks by criminal groups and to prevent infiltration by hostile organizations. The concept of cybersecurity covers a wide range from the protection of interactions in information technologies to security cooperation between the state and the private sector. The effectiveness of cybersecurity depends on the government's ability to coordinate security measures with the private sector against common threats and the flexibility demands of the public and private sectors. For example, factors such as "compliance requirements" in the financial sector can greatly affect the success of cybersecurity measures. However, being able to effectively respond to new challenges brought about by technological advances requires continuous effort and adaptation in the field of cybersecurity (Sulich et al., 2021, 21-22). One of the most important factors that prevent organizations or businesses from focusing on major corporate goals is the lack of a clear framework to protect all assets, processes, and resources. Effective implementation of a cybersecurity strategy depends on guidelines such as the right cybersecurity framework and industry-specific best practices. A cybersecurity framework covers guidelines that include security standards, practices, and best practices and is critical for protecting against cyber threats and managing the security of the organization (Syafrizal et al., 2020: 417). Cybersecurity plays a critical role in preventing cyberattacks and minimizing the potential damages of these attacks. While operational capabilities generally focus on reducing the number of incidents, building cyber resilience aims to minimize potential damages by effectively protecting companies' important information assets and business interests. In addition, security investments encourage companies to innovate; because protecting new inventions from competitors provides a competitive advantage in the long term. For example, Apple gains consumers' trust by prioritizing security and privacy in mobile devices and cloud services, leading to the preference for its products. Security innovation allows companies to increase their revenue opportunities and differentiate themselves in the market (Kosutic and Pigni, 2022: 29-30). Cybersecurity is a technology field that protects our digital assets from unauthorized access, malicious use, and abuse. These threats can range from groups attacking information systems over the internet to various computing devices such as smartphones, smart TVs, and laptops. As our dependence on computing devices increases, the importance of cybersecurity is also growing. Therefore, standardization of cybersecurity is a critical necessity today. Cybersecurity is considered an integrated digital defense mechanism that protects everyone from individuals to businesses, from educational institutions to governments. This field aims to protect digital systems, networks, equipment, and information from any unauthorized access, modification, disclosure, interruption, monitoring, wiretapping, or destruction (Hamdani et al., 2021: 2). Cybersecurity includes a variety of applications, technologies, and processes to protect the data, networks, programs, and devices of individuals and organizations. Financial, corporate, government, military, and medical organizations cooperate to protect sensitive personal, financial, and intellectual property information. Unauthorized access to such information is associated with serious consequences; therefore, strict authorization is necessary. Increasing business transactions and data transfers further emphasize the need for this protection. Cybersecurity also includes the protection of information storage and processing systems. The increase in cyberattacks today increases the responsibility to protect financial records, health information, and national security data. Cybersecurity strategies help prevent malicious attacks and protect the functioning of devices by taking measures to protect these data and systems (AL-Hawamleh, 2023: 801-802).

3. Corporate Trust

Corporate trust is a concept that plays a fundamental role in establishing effective communication and cooperation among employees. This trust reflects the expectations and trust levels of employees regarding relationships and work processes within the organization. Organizational trust includes the trust that individuals have not only in each other but also in their managers. A high level of corporate trust increases the commitment and loyalty of employees to both their organization and their colleagues. This environment of trust encourages cooperation and strengthens communication among employees, thus ensuring that work processes are carried out more effectively. In addition, a healthy environment of trust positively affects employee motivation and overall job performance. Establishing and maintaining trust is a critical strategic element for the long-term success of organizations. Creating a safe work environment not only increases the productivity of current employees, but also strengthens the reputation of the organization and provides a solid

foundation for its future success (Zanabazar, 2022: 2). Corporate trust is defined as the development of positive expectations regarding intentions and behaviors by multiple organization members based on factors such as roles, relationships, experiences, and interdependencies within the organization. This concept refers to a broad assessment of the overall trustworthiness of an organization and the perception of trust and support provided by the employer. Research on trust is generally addressed at two different levels: micro and macro levels. Micro-level research focuses on examining the feelings of trust among individuals and their perceptions of trustworthiness. This approach provides an in-depth understanding of individual relationships and personal trust beliefs. On the other hand, macro-level research is aimed at assessing the atmosphere of trust and the general climate of trust throughout the organization. Studies conducted at this level address the dynamics of trust among all members of the organization and the general climate of trust. The combination of research at these two levels allows for a comprehensive understanding of both individual feelings of trust and the organizational climate of trust and allows for a better assessment of the effects of trust on organizational success (Joo et al., 2023: 6). Corporate trust is the cornerstone of establishing healthy and productive relationships both among employees and between employees and the organization. When trust is lacking, maintaining these relationships becomes more costly. Trust plays a critical role, especially in situations where the parties look after the interests of the other party rather than their own. In this context, trust stands out as a determining factor not only in business relationships but also in the overall efficiency and success of the organization (Jarrar and Ibrahim, 2021: 1-5). Creating a healthy work environment lays the foundation for a positive organizational culture, which in turn depends largely on trust among organizational members. Corporate trust has a long history in management literature and is at the core of effective organizational management. This trust plays a critical role in leadership and teamwork processes and is an indispensable element for the success of the organization (Aruoren et al., 2023: 20).

The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST), serves as a comprehensive guide to help organizations effectively manage information security risks. This framework aims to support organizations in developing protection strategies against cyber threats and enhancing their operational resilience (NIST, 2018: 4–6). Fombrun's definition of reputation refers to the perception of reliability and prestige that a company holds in the eyes of its stakeholders. There are two key factors that influence a company's ability to generate value from its reputation: the first is the strategy the company pursues, and the second is its practices in shaping corporate identity and building its image. A strong reputation plays a crucial role in ensuring the sustainable success of an organization (Fombrun, 1996). The trust model proposed by Mayer, Davis, and Schoorman (1995) explains the dynamics of trust between individuals and organizations by identifying three core components of trust: ability, integrity, and benevolence (Mayer et al., 1995: 717–725). This conceptual framework provides an important foundation for understanding how cybersecurity practices impact an organization's reputation and the trust of its employees.

Trust plays a critical role in economic, political, and social organizations. Especially at the organizational level, trust is now considered a basic feature, and according to research, it is a vital factor in the productivity and commitment of the workforce. Trust can be defined as an environment created by managers and is necessary for an effective work process. In the absence of trust, employees cannot perform their jobs effectively and efficiently. Establishing and maintaining trust in businesses is of great importance in terms of cooperation and productivity. The success of organizations is directly related to creating a trusting atmosphere and maintaining this trust. Trust supports employees to be motivated, think innovatively, and achieve the goals of the organization more effectively (Hanif et al., 2020: 76). The concept of trust essentially consists of elements such as truthfulness, reliability, honesty, and faith. These elements are of critical importance for the smooth functioning of relationships and collaborations within the organization. These basic qualities ensure that organizational interactions take place healthily and effectively (Abun et al., 2022: 112-113). Trust is the willingness of a person or organization to be vulnerable without having the capacity to monitor and control another person or organization in the expectation that they will perform certain actions. This expectation is based on the honesty, intentions, and competence of the other party. Trust is built on relationships of mutual dependency and requires internal harmony between the parties. Distrust can arise from real differences in knowledge, experience, or values and does not always mean an irrational or mindless response. Trust is a fragile trait; it is built slowly but can be destroyed quickly. Distrust can cause breakdowns in communication and have costly consequences. In conclusion, trust and distrust are complex emotional and psychological concepts that have profound effects on human relations and organizational interactions. When managed well, trust can pave the way for cooperation and success, while distrust can weaken relationships and have negative consequences. Therefore, increasing trust and reducing distrust are of strategic importance for both individuals and organizations (Kebede et al., 2022: 3). The role of organizational trust in achieving organizational success

is unavoidable. Trust is a critical element for an organization because it offers many important advantages. Especially in times of crisis or difficulty, it has a decisive effect on how employees perceive and react to these situations. When a safe environment is created, employees are more willing to cooperate, communication is more open and effective, and solution-oriented thinking is encouraged. In addition, in a safe work environment, employees are more committed and motivated to their organisation's goals, which increases overall organizational performance. On the other hand, in the absence of trust, employees may be skeptical or resistant to the organization's decisions and strategies. This can negatively affect the organization's ability to manage the crisis, especially in times of crisis. As a result, organizational trust not only helps to carry out daily tasks but also plays an important role in staying strong in crises and ensuring long-term success (Pranitasari, 2020: 77-78). Corporate trust plays a vital role in maintaining an organisation's long-term stability and protecting its members' well-being (Lambert et al., 2024: 4-5). Corporate trust forms the cornerstone of relationships within an organization and is an important element that directly affects business performance. Corporate trust, which is often associated with positive work psychology emotions, also affects job performance. Trust can occur in various forms, including coworker trust, supervisor trust, and management trust. Coworker trust refers to the trust that individuals feel that their coworkers are honest and care about their well-being. Managerial trust is related to the perception of the manager as fair and fulfilling his/her promises. Management trust, on the other hand, includes the expectation that management will be helpful or not harm employees. Providing these types of trust can increase employee participation, satisfaction, and commitment (Lambert et al., 2022:27-28). Organizational trust, as a complex social and psychological phenomenon, is usually examined from two main perspectives: "inter-organizational trust" and "intraorganizational trust." This concept includes the general perceptions of organizational members about management's decisions and practices, as well as their experiences of how organizational rules and regulations are implemented. When employees believe that their organization is fair, their trust in their organization increases, and this trust develops a belief that they will be provided with fair returns in material and moral terms. This sense of trust encourages employees to take on more responsibility beyond their job descriptions (Tan et al., 2021: 524).

In the business world, corporate trust is a critical element in terms of conducting business in an orderly and effective manner. Employees' trust in each other ensures that information sharing is healthy and efficient, and this trust becomes even more important, especially in changing business conditions. An employee or manager with a high level of corporate trust shares information openly increases their commitment to the organization, and this positively affects business performance. In addition, gaining the trust of internal and external customers strengthens trust in business performance. Organizational trust is an indicator of the trust and belief an organization has in its employees. Even in management environments where uncertainty and change are intense, encouraging consistent organizational behavior and cooperation helps maintain an environment of trust (Kim, 2020: 115). In today's corporate world, ensuring organizational performance, efficiency, and effectiveness is of critical importance. In this context, the concept of corporate trust plays a major role based on the level of trust that all employees have in each other and their organizations. Corporate trust emerges as a fundamental factor in the success of rules, methods, goals, and objectives. This concept refers to the mutual trust and respect that exists between members of an organization and enables the effective execution of cooperation, information sharing, and problem-solving skills. In the absence of corporate trust, the risk of uncertainty, conflict, and inefficiency among employees increases. In environments where trust is insufficient, employees may feel vulnerable and may not trust others. This situation can make cooperation and teamwork difficult, prevent information sharing, and, as a result, negatively affect organizational performance. Corporate trust is a critical component for the healthy functioning of an organization. Creating an environment of trust, enables employees to feel comfortable, share their ideas freely, and focus on the goals of the organization (Alhamad et al., 2022: 3). Corporate trust is a critical element for productive and long-term employee-employer relationships. This environment of trust forms a fundamental building block for organizations to achieve sustainable success and effectiveness. A safe working environment increases employee motivation, encourages cooperation and innovation, and thus strengthens the competitiveness of the organization. Therefore, it is of great importance for organizations to develop strategic approaches to support and maintain trust (Silva, 2023: 95). Corporate trust is closely related to many important factors such as effectiveness, productivity, interpersonal citizenship behaviors, proactive attitudes, and job satisfaction within an organization. The existence of an environment of trust encourages teamwork and increases performance levels. In addition, corporate trust is one of the cornerstones of the leader-follower relationship; this relationship highlights the importance of trust and justice that leaders have for their employees. For employees, a sense of trust also brings with it a belief that the organization will be beneficial in every way (Widanti and Sunaryo, 2022: 54). As a result, corporate trust is a critical factor for the development and strengthening of human relations. It creates

deep effects on employees' satisfaction, commitment, and job performance. Trust in the organization's decisions and policies greatly affects employees' beliefs in the organization's goals and their motivation towards these goals. Therefore, corporate trust is an element of strategic importance for long-term success (Sadq et al., 2020: 2642).

4. Corporate Reputation

Corporate reputation does not have a common definition as it is defined in different ways in various disciplines. In general, it is seen as a perceptual representation that expresses the general attractiveness of a company's past actions and future expectations for all key components of the firm. Corporate reputation is considered a characteristic of an organization and reflects how stakeholders perceive how "good" the firm is (Javed et al., 2019: 1399). Corporate reputation is the most valuable intangible asset of the company and forms the basis of sustainable competitive advantage. A strong corporate reputation strengthens the company's relationships with its stakeholders; ensures that loyal customers are willing to pay high prices, attracts talented job candidates, and increases the desire of current employees to stay with the company. Therefore, corporate reputation can affect the value of the company. In addition, corporate reputation is defined as a concept that reflects the expectations of different stakeholders about the company's ability to satisfy their interests (Pérez-Cornejo et al., 2019: 1252-1253). Corporate reputation refers to the long-term evaluation of a company's behavior and outcomes by stakeholders. In contrast, a company's corporate image is shaped by customers' short-term perceptions and evaluations of its activities and communication (Kamal et al., 2022: 72). Therefore, corporate reputation is the result of a legitimation process in which various audiences evaluate a company's characteristics and past performance to form expectations about possible future behavior (Pérez-Cornejo et al., 2023: 284). Corporate reputation can be defined as the sum of the information and feelings a person has about an organization (Afandi et al., 2021: 43).

Corporate reputation is a very dynamic subject of study in the field of organizational management. Organizations usually build this reputation over time or may gain or lose popularity in a particular sector. However, corporate reputation is constantly changing; any positive or negative development can cause the reputation to improve or deteriorate. Corporate reputation plays an important role in various fields such as organization theory, strategic management, marketing, accounting and finance, communication, and economics (Zeesahn et al., 2020: 188). Managers can gain a competitive advantage for organizations by using corporate reputation as a strategy. Corporate reputation is a critical strategic tool that businesses use to achieve their strategic goals (Islam et al., 2021: 128-129). The company's identity is usually reflected through communication activities with customers, which is directly related to the company's image. The company's image is an evaluation formed by stakeholders based on their direct experiences with the company. Communication styles and symbols provide information about the company's activities compared to its competitors. A positive corporate image, formed through effective communication, can contribute to the development of a strong corporate reputation over time. This study defines a company's reputation as an evaluation resulting from direct and indirect experiences provided to customers and other stakeholders through technology-based services (Ikhsan and Simarmata, 2021: 562-563). Corporate reputation refers to the admiration and respect a person has for an organization at a given time. While corporate image reflects the company's current visual and communicative presentation, corporate reputation becomes an important part of brand value by encompassing stakeholders' long-term judgments and experiences. Factors that indicate brand and product performance, such as customer loyalty, sales, and profit, can be affected by corporate reputation. Corporate reputation does not only stem from the company's unique capabilities or expertise; it is also a result of the complex interactions the firm establishes with its stakeholders. Many factors, from marketing strategies to employment policies, can affect a company's reputation (Caviggioli et al., 2020: 877-878).

Corporate image is the overall impression formed through recent customer interactions and communication, while corporate reputation develops over time as a result of accumulated stakeholder experiences and evaluations. Once a brand reputation is formed in the mind of the customer, it does not remain fixed; this reputation can change over time as customers respond to new signals from the brand (Lee and Hur, 2024: 2). Corporate reputation is a valuable asset that has a great impact on consumers' responses to products. Companies generally offer various reputation-building strategies to consumers to create a positive reputation and benefit from the advantages provided by this reputation (Chen et al., 2024: 2). Therefore, the reputation of an organization is directly related to the decisions it has made and the actions it has taken in the past. Reputation is an asset in itself, beyond being an element reflecting the history of a company (Ion et al., 2021: 523). Corporate reputation is considered one of the most valuable intangible assets of organizations because it has the potential to increase or decrease the value of an organization. A strong corporate reputation provides the

organization with a sustainable competitive advantage, which increases the likelihood of achieving goals among various stakeholders, from customers to business leaders, suppliers, and current/potential employees. Corporate reputation is shaped by how both internal and external stakeholders perceive the organization. While image can vary among different audiences based on recent interactions, reputation is a more stable construct built over time through repeated and consistent experiences. An organization's reputation is formed through the emotional bonds that stakeholders establish with employees, and these bonds are strengthened through formal and informal interactions. To increase the support of internal and external stakeholders, it is of great importance that these emotional bonds are compatible with the organization's corporate identity (Potgieter and Doubell, 2020: 110). Therefore, corporate reputation is a collective reflection of stakeholders' multidimensional individual evaluations of a company. These evaluations are based on perceptions of the company's past actions and future expectations compared to competitors. Since it is directly related to business success, companies need to monitor their reputation regularly as part of the reputation management process (Baumgartner et al., 2020: 3).

5. Methodology

In this study, where the relationship between cybersecurity, corporate trust, and corporate reputation was investigated, some descriptive statistics, factor analyses, reliability analyses, simple linear regression analyses, and correlation analyses were performed on the survey data of 252 participants who were found to be suitable for analysis, using the SPSS (version 25) and AMOS (version 24) programs (IBM Corp., 2017).

Before starting the research process, approval was obtained from the Istanbul Nişantaşı University Ethics Committee. Our study titled "The Relationship Between Cyber Security, Corporate Trust and Corporate Reputation in Businesses", which was applied on 21/08/2024, was evaluated at the ethics committee meeting numbered 2024/08 dated 22/08/2024 and the committee unanimously decided that the research was ethically appropriate. In this context, data collection procedures were carried out in full compliance with ethical rules during the research process.

5.1. Research Population, Sampling and Data Collection Method

The businesses in the Marmara region constitute the study's population. Convenience sampling was used. Data deemed suitable for analysis were collected from 252 participants using face-to-face and online survey methods. Survey data were collected between August 2024 and April 2025. The required sample size was calculated to be 123 at an effect size of 0.15 (a medium effect size default value determined by the G*Power program), with 95% power and a 0.01 significance level, using the G*Power program version 3.1.9.7 (Faul et al., 2009; Faul et al., 2007).

5.2. Scales of the Research

The survey method was used to collect the data and a 5-point Likert-type scale was preferred. A pilot study was conducted with 86 participants to test the clarity and applicability of the scales, and the results supported the reliability and validity of the scales. The obtained data were analyzed in detail with the SPSS and AMOS programs. This study used a scale of 11 items developed by Howard (2018) to measure cybersecurity. Cybersecurity questions are coded as "CSecurity". To assess corporate trust, a scale consisting of 6 items used in higher education institutions by Dalati, Raudeliūnienė, and Davidavičienė (2017) was used. This scale aims to measure the trust of employees in their institutions and was applied as a data collection tool in our research. Corporate trust questions are coded as "CTrust". In addition, a scale consisting of 8 items developed by Feldman, Bahamonde, and Velasquez Bellido (2014) was used to determine the level of corporate reputation. This scale aims to measure the general perceptions of the participants about the institutions by addressing corporate reputation in a multidimensional manner. Corporate reputation questions were coded as "CReputation".

5.3. Research Model and Hypotheses

Figure 1. shows the research model.

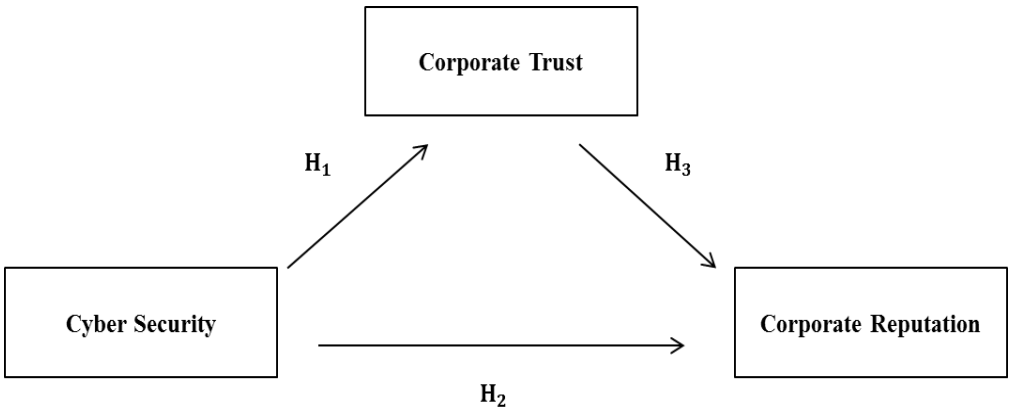

Figure 1: Research Model

The hypotheses of the research are as follows;

H_1: Cybersecurity has a positive and significant effect on corporate trust.

H_2: Cybersecurity has a positive and significant effect on corporate reputation.

H_3: Corporate trust has a positive and significant effect on corporate reputation.

6. Results

6.1. Demographic Analysis Results

The demographic analysis results of the participants in the study are given in Table 1.

Table 1: Demographic analysis results

Gender					**Activity Limit**				
	Frequency	%	Valid %	Cumulative %		Frequency	%	Valid %	Cumulative %
Female	96	38,1	38,1	38,1	National	102	40,5	40,5	40,5
Male	156	61,9	61,9	100	Inter national	150	59,5	59,5	100
Total	252	100	100		Total	252	100	100	
Age					**Field of Activity**				
	Frequency	%	Valid %	Cumulative %		Frequency	%	Valid %	Cumulative %
18-25 age	23	9,1	9,1	9,1	Service	143	56,7	56,7	56,7
26-36 age	127	50,4	50,4	59,5	Production	109	43,3	43,3	100
37-46 age	5	2	2	61,5	Total	252	100	100	
47 and above	97	38,5	38,5	100	**Department**				
Total	252	100	100			Frequency	%	Valid %	Cumulative %
Educational Status					Production	67	26,6	26,6	26,6
	Frequency	%	Valid %	Cumulative %	Accounting	46	18,3	18,3	44,8
University	152	60,3	60,3	60,3	Sales	54	21,4	21,4	66,3

Master's degree	91	36,1	36,1	96,4	R&D	76	30,2	30,2	96,4
Doctorate	9	3,6	3,6	100	Other	9	3,6	3,6	100
Total	252	100	100		Total	252	100	100	

When the gender distribution of individuals participating in the survey is examined, it is observed that 61.9% of them are male and 38.1% are female. The fact that the male participant rate is higher than that of females may indicate that males participate more, especially in certain sectors, or that males have a higher desire to participate in the sample group in which the survey was conducted.

When the ages of individuals in the data set are examined, it is seen that the majority of the participants are concentrated in the 26-36 age range. In addition, the rate of the 37-46 age group is at a lower level.

When evaluated in terms of education level, university graduates have the highest share (60.3%). This shows that the majority of the participants have completed a basic higher education level. Doctoral graduates constitute the lowest rate in the group with a share of 3.6%.

The activity limits of the organizations were evaluated based on their geographical scope and the regions they serve. According to the analyzed data, there are 59.5% organizations operating at an international level. These organizations provide services in various provinces throughout Turkey and develop comprehensive activities for the market. There are 40.5% of companies operating at a national level.

The sectoral distribution of participants in terms of field of activity is as follows: the service sector has the highest share with 56.7%. The rate of participants in the production sector is 43.3%.

When the department-based distribution is examined, the highest rate belongs to the R&D department (30.2%). This situation shows that the analyzed companies attach importance to innovation and product development processes and invest in research and development activities to gain a competitive advantage. Especially for companies operating in the international market, R&D is considered a critical element for sustainable growth and global competition. The production department ranks second with a rate of 26.6%, indicating that companies attach importance to production capacity and management of production processes in operational processes. The strong representation of the production department reveals that companies work based on goods and products and that production-based business models still have significant weight. The sales department is at a rate of 21.4%. This rate shows that companies attach importance to marketing and customer relationship management processes and that sales teams play critical roles in the competitive environment in the market. The representation of the accounting department with 18.3% shows that functions such as financial management, budget control, and financial reporting are carried out within a standard structure within the organization. Other departments have a low rate of 3.6%.

6.2. Normality Test Analysis Results

Table 2 includes kurtosis, skewness, means, and standard deviation values.

Table 2: Kurtosis, skewness, means, and standard deviation values

Statistics			
	CSecurity	CTrust	CReputation
N	252	252	252
Mean	3,0380	3,9894	3,0898
Std. Deviation	,99184	,50397	,87179
Skewness	-,107	-,195	-,008
Kurtosis	-1,279	-,778	-1,330

Table 2 shows the skewness and kurtosis values, means, and standard deviations of the scales used in the study. The Mean section provides the means of the variables, the Std. Deviation section provides the standard deviations of the variables and N provides information about the number of entered data. The skewness and kurtosis values were examined to determine whether the data conformed to the normal distribution. Within the scope of the normality test applied to determine whether the data set had a normal distribution, it was determined that the skewness and kurtosis values varied between -1.330 and -.008 and that there were no extreme values in the data set. The fact that the skewness and kurtosis values were between +1.5 and -1.5 indicates that the data was normally distributed (George and Mallery, 2016).

6.3. Factor Analysis Results

Table 3 shows the results of the explanatory factor analysis.

Table 3: Exploratory factor analysis results

Rotated Factor Matrix			
	Factor		
	1	2	3
CReputation 6	,725		
CReputation 7	,674		
CReputation 4	,628		
CReputation 8	,622		
CReputation 2	,617		
CReputation 5	,605		
CReputation 1	,597		
CReputation 3	,533		
CSecurity3		,659	
CSecurity1		,627	
CSecurity2		,623	
CSecurity4		,596	
CSecurity8		,558	
CSecurity6		,552	
CSecurity7		,520	
CTrust4			,651
CTrust6			,601
CTrust3			,567
CTrust2			,535
CTrust1			,517
CTrust5			,515
Extraction Method: Maximum Likelihood. Rotation Method: Varimax with Kaiser Normalization.			
a. Rotation converged in 6 iterations.			

A strong conceptual basis is needed to support the assumption that a structure exists before factor analysis can be performed. A statistically significant Bartlett's test of sphericity (sig. 0.50) indicates that there are sufficient correlations among the variables to proceed. The values for the measure of sampling adequacy should exceed .50 for both the overall test and each variable; variables with values less than .50 should be individually excluded from the factor analysis (Hair et al., 2019: 137).

The results of the explanatory factor analysis are given in Table 3. The factor analysis was performed with the maximum likelihood and varimax options selected. The factor analysis was first analyzed separately for each scale. As a result of the separate factor analysis, items 9, 5, 11, and 10 from the cybersecurity scale questions, which were found to be lower than 0.50, were removed from the scale in order. In the factor analysis results performed on the other scales, it was determined that each scale item was above 0.50.

As a result of the explanatory factor analysis performed on all scales together, 3 factors were formed. Table 4 shows the KMO and Bartlett's test results.

Table 4: KMO and Bartlett's test results

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,919
Bartlett's Test of Sphericity	Approx. Chi-Square	2011,161
	df	210
	Sig.	,000

As seen in Table 4, the Kaiser Meyer Olkin (KMO) coefficient was calculated as .919 as a result of the analysis conducted to test the suitability of the research sample size for factor analysis. The data set is suitable for factor analysis to the extent that the Kaiser Meyer Olkin (KMO) value is greater than 0.60 (Noor Arzahan et al., 2024: 14). Since this KMO = .919>0.60 is obtained, it is stated that it is a sufficient and reliable value to perform factor analysis. As a result of the Bartlett test, it was determined as (p=.000<.001), and it was accepted that there was a relationship between the variables. Table 5 shows the total variance analysis results.

Table 5: Total variance analysis results

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	7,357	35,033	35,033	6,807	32,413	32,413	3,714	17,687	17,687
2	1,820	8,668	43,701	1,185	5,641	38,055	3,071	14,622	32,308
3	1,728	8,228	51,929	1,220	5,810	43,865	2,427	11,557	43,865
4	,882	4,200	56,129						
5	,856	4,075	60,204						
6	,800	3,809	64,013						
7	,744	3,541	67,554						
8	,718	3,417	70,971						
9	,680	3,239	74,210						
10	,624	2,974	77,184						
11	,592	2,821	80,005						
12	,574	2,733	82,738						
13	,505	2,407	85,145						

14	,486	2,315	87,460						
15	,465	2,215	89,675						
16	,435	2,069	91,744						
17	,417	1,986	93,730						
18	,384	1,829	95,559						
19	,334	1,591	97,150						
20	,310	1,478	98,628						
21	,288	1,372	100						
Extraction Method: Maximum Likelihood.									

An eigenvalue above 1 indicates that the relevant factor explains more common variance than a single variable and therefore can be considered significant. In addition, a factor's variance between 40% and 60% reveals that the factor analysis is at an acceptable level in terms of structural validity (Karaman, 2023). This study determined that the 3 sub-dimensions used in the scale explained 43.865% of the total variance. The eigenvalues of the three sub-dimensions were greater than 1. The first factor explained 17.687% of the total variance (eigenvalue 3.714), the second factor explained 14.622% of the total variance (eigenvalue 3.071), and the third factor explained 11.557% of the total variance (eigenvalue 2.427).

Confirmatory factor analysis was also conducted using the AMOS program. As a result of the analysis, CMIN/DF was determined as 1.393, CFI as 0.961, NFI as 0.875, PNFI as 0.775, TLI as 0.956, RMSEA as 0.040, and SRMR as 0.048. All values were found to be acceptable levels (Schumacker and Lomax, 2010).

6.4. Reliability Analysis and Validity Analysis Results

Table 6 shows the reliability analysis results.

Table 6: Reliability analysis results

	Cronbach's Alpha	N of Items
CSecurity	,837	7
CTrust	,777	6
CReputation	,879	8

A Cronbach's Alpha value between .7 and .8 is considered acceptable (Field, 2018). According to the reliability statistics in the SPSS analysis, Cronbach's Alpha values for all three sub-dimensions were above .7; this shows that the internal consistency of the scales is sufficient and reliable. The Cronbach's Alpha value of the cybersecurity sub-dimension is .837, the Cronbach's Alpha value of the corporate trust sub-dimension is .777, and the Cronbach's Alpha value of the corporate reputation sub-dimension is .879, indicating that each dimension is highly reliable. According to the reliability test results, it is revealed that all questions in the scale are perceived correctly and in the same direction by the participants. Therefore, it shows that the scales used make consistent and valid measurements. Table 7 shows the Heterotrait-Monotrait Ratio of Correlations (HTMT), Average Variance Extracted (AVE), and Composite Reliability (CR) analysis results. Master Validity Tool was used in the analysis (Gaskin, James, and Lim (2019).

Table 7: HTMT, AVE, and CR analysis results

	CR	AVE	CSecurity	CReputation	CTrust
CSecurity	0,836	0,426			
CReputation	0,879	0,477	0,679		
CTrust	0,777	0,369	0,552	0,572	

It is understood that HTMT analysis results being less than 0.85 are acceptable for discriminant validity (Franke and Sarstedt, 2019). If the CR value is greater than 0.60, convergent validity is acceptable even if the AVE value is less than 0.50 (Huang et al., 2013; Lam, 2012).

6.5. Correlation Analysis Results

Table 8 shows the correlation results.

Table 8: Correlation analysis results

		CSecurity	CTrust	CReputation
CSecurity	Pearson Correlation	1	,446**	,587**
	Sig. (1-tailed)		,000	,000
	N	252	252	252
CTrust	Pearson Correlation	,446**	1	,474**
	Sig. (1-tailed)	,000		,000
	N	252	252	252
CReputation	Pearson Correlation	,587**	,474**	1
	Sig. (1-tailed)	,000	,000	
	N	252	252	252

**. Correlation is significant at the 0.01 level (1-tailed).

A value of 0.30 is considered a medium effect size, and a value of 0.50 is considered a large effect size (Cohen, 1988). The findings of the correlation analysis conducted within the scope of the research were evaluated comprehensively. The given Pearson correlation table shows the relationships between three variables: cybersecurity, corporate trust, and corporate reputation. The correlation coefficient values indicate the linear relationship between the variables. It indicates a moderately positive (r=.446) and significant (p<.001) positive relationship between cybersecurity and corporate trust. Similarly, a moderately positive (r=.587) and significant (p<.001) relationship was found between cybersecurity and corporate reputation. In other words, the participants' cybersecurity and corporate reputations increase together with a moderately positive and significant relationship. A moderately positive (r=.474) and significant (p<.001) relationship was found between corporate trust and corporate reputation. In this context, all three relationships are statistically significant as a result of the research, because the p-values are .000 and are below the .001 level. These results reveal that all three variables are positively related to each other and that there is a significant connection.

6.6. Regression Analysis Results

Table 9 shows the regression analysis results for H_1.

Table 9: Regression analysis results for H_1

Independent Variable	R	R^2	F	B	Std. E.	β	t	p
CSecurity	,446	,199	62,147*	,227	,029	,446	7,883	,000
Dependent Variable: CTrust								
*=p<,001, Std. E.= Standart Error								
Durbin-Watson=1,682, Tolerance=1,000, VIF=1,000								

Hypothesis analyses were performed using simple linear regression analysis.

H_1: Cybersecurity has a positive and significant effect on corporate trust.

In the simple linear regression analysis where one dependent and one independent variable were considered, the significance level was determined as Sig.= .000. This result shows that there is a statistically significant relationship between the two variables and that the analysis is valid. In addition, the F test value above 1

supports that the model is statistically significant. The R coefficient showing the level of relationship between the variables was found as .446, which shows that there is a strong relationship between the two variables. The coefficient of determination (R^2) was determined as .199, and it is understood that the independent variable explains 19.9% of the total change on the dependent variable. The effect of the independent variable is positive, and the effect of cybersecurity on corporate trust is 22.7% (B=.227). An interpretation can be made about the general suitability of the regression model with the F test value. In order to evaluate the explanatory power, the p-value must be less than 0.05 (Amalia and Safitri, 2025). Durbin Watson value being between 1 and 3 and VIF (Variance Inflation Factor) and Tolerance values being equal to 1 are considered acceptable for analysis (Field, 2018). Durbin Watson, VIF and Tolerance values were found acceptable as a result of analysis.

As a result, according to the regression analysis data, it is seen that cybersecurity has a direct and positive effect on corporate trust. The analysis reveals that the effect of cybersecurity on the dependent variable, corporate trust, is statistically significant (p<.001). Table 10 shows the regression analysis results for H_2.

Table 10: Regression analysis results for H_2

Independent Variable	R	R^2	F	B	Std. E.	β	t	p
CSecurity	,587	,344	131,120*	,516	,045	,587	11,451	,000
Dependent Variable: CReputation								
*=p<,001, Std. E.= Standart Error								
Durbin-Watson=1,348, Tolerance=1,000, VIF=1,000								

H_2: Cybersecurity has a positive and significant effect on corporate reputation.

Hypothesis analyses were performed using simple linear regression analysis.

The significance value of the simple linear regression model in which one dependent and one independent variable were analyzed was Sig. =,000. In other words, a significant relationship was found between both variables and the analysis was valid. The F test value being more than 1 also shows that the model is significant. The R statistic showing the correlation coefficient between the variables was found to be,587. In this case, we can say that there is a good relationship between the two variables. When the results of the research are examined, it is seen that the coefficient of determination is (R2 =,344). In other words, the explanatory power of the independent variable on the dependent variable is 34.4%. The effect of the independent variable on the dependent variable is positive and the effect of cybersecurity on corporate reputation is 51.6% (B =,516). Durbin Watson, VIF and Tolerance values were found acceptable as a result of analysis.

When the regression analysis results are examined, it is seen that the cybersecurity factor has a direct and positive effect on corporate reputation. The regression analysis conducted to evaluate the effect of cybersecurity on the dependent variable, corporate reputation, was found to be statistically significant (p<.001). Table 11 shows the regression analysis results for H_3.

Table 11: Regression analysis results for H_3

Independent Variable	R	R^2	F	B	Std. E.	β	t	p
CTrust	,474	,224	72,330*	,819	,096	,474	8,505	,000
Dependent Variable: CReputation								
*=p<,001, Std. E.= Standart Error								
Durbin-Watson=1,044, Tolerance=1,000, VIF=1,000								

H_3: Corporate trust has a positive and significant effect on corporate reputation.

Hypothesis tests were performed using the simple linear regression analysis method. In this linear regression model where one dependent and one independent variable were evaluated, the significance level was obtained as Sig.=,000. This situation shows that there is a significant relationship between the two variables and reveals the validity of the analysis. In addition, the F test value above 1 supports that the model is statistically

significant and strong. The R-value, which expresses the correlation coefficient between the variables, was determined as,474, and this result shows that there is a significant and positive relationship between the two variables. According to the research findings, the coefficient of determination (R^2) was determined as,224, and in this context, it was understood that the independent variable explained 22.4% of the total variance on the dependent variable. The effect of the independent variable was positive, and the effect of corporate trust on corporate reputation was 81.9% (B=,819). When the regression analysis results were evaluated, it was seen that the corporate trust variable had a direct and positive effect on corporate reputation. Durbin Watson, VIF and Tolerance values were found acceptable as a result of analysis.

As a result of the regression analysis conducted to examine the effect of corporate trust on the dependent variable, corporate reputation, it was determined that this relationship was statistically significant (p<001).

7. Conclusion

This study examines the relationship between cybersecurity, corporate trust, and corporate reputation, which has not been previously examined in the literature. In today's digitalized business world, cybersecurity, corporate trust, and corporate reputation are not considered independent of each other but have become intertwined and have become strategically important for the sustainable success of institutions. Institutions are obliged to protect both their physical assets and digital systems from a strategic perspective. It should not be forgotten that this protection approach should not be limited to purely technical security measures; it is also important to support it with a transparent and reliable corporate structure that reinforces the sense of trust of employees. Comprehensive defense strategies being developed against digital attacks directly affect the reputation of the institution by protecting data security. In this respect, all activities to be carried out by institutions or organizations for cybersecurity make a significant contribution to the strengthening of corporate trust and corporate reputation in the long term.

Today, it has become a necessity for institutions or organizations to strategically protect their digital assets. An attack by malicious actors operating in the cyber environment is associated not only with financial losses for the institution but also with a significant decline in the trust of customers, who are vital to the institution's survival. As a result, the corporation's reputation can be directly affected. Therefore, this situation can threaten the institution's long-term existence and competitiveness. Therefore, institutions must take precautions against cyber attacks by acting with a proactive defense approach and strengthening their corporate reputation.

Corporate reputation is one of the fundamental dynamics that determine a company's position in the market and its sectoral reliability. Organizations with corporate reputations can achieve sustainable financial success by gaining the trust of their stakeholders and customer loyalty. Corporate reputation is shaped by both internal company achievements and external perceptions. The development of cybersecurity applications is important for corporate reputation, and there is a strong mutual interaction between them.

Corporate trust, which forms the basis of the internal functioning of the institution, directly affects the relationships, cooperation, and commitment between employees. Being prepared for digital threats is not only related to the level of awareness and trust environment of employees but also to technical measures. Therefore, corporate trust stands out as a fundamental element in the adoption and sustainability of cybersecurity awareness within the institution.

In conclusion, cybersecurity, corporate trust, and corporate reputation are the fundamental building blocks that complement and strengthen each other in achieving strategic success for contemporary organizations. For institutions, addressing these elements in an integrated manner provides effective protection against digital threats while also enabling the construction of a strong brand value and sustainable internal structure. Therefore, in their digital transformation processes, institutions need to adopt a holistic development process that will encompass not only their technological infrastructure but also their corporate reputation and internal trust structures.

The findings of the research are based on regression analyses and correlation tests examining the relationships between cybersecurity, corporate reputation, and corporate trust. The results show that cybersecurity has a positive and significant effect on both corporate trust (r=,446, p<,001) and corporate reputation (r=,587, p<,001). In addition, corporate trust was found to have a positive and significant effect on corporate reputation (r=,474, p<,001). In some studies in the literature, it has been concluded that cybersecurity has a positive and significant effect on corporate security performance (Berlilana et al., 2021), e-operational efficiency (Basri, 2023), e-logistics performance (Nuseir et al., 2024), minimizing operational risks (Ali et al., 2025), financial performance (Aminu, 2024), and the relationship between strategic intelligence and increasing competitive

advantage (Jebril et al., 2023). Studies in the literature appear to focus on performance, efficiency, risk minimization, competitive advantage, etc. This study provides some insight into the interaction between cybersecurity and corporate trust and corporate reputation. It is thought that the results of this study and the method used can provide useful information for researchers' future studies on cyber security, corporate trust, and corporate reputation.

The method (quantitative), tool (SPSS and AMOS), sample, scales used, time of the analysis, and the opinions of the individuals participating in the analysis constitute the limitations of this study. In future studies, this research can be repeated in different countries, and regions, with different methods and tools, and different factors can be added and analyzed with different effects. In future studies, evaluating the effects of variables in the digital transformation process on cybersecurity perceptions will make a significant contribution to increasing knowledge in this area.

References

Abun, D., Fredolin, J. P., Galat, M. A., & Lazaro, J. R. (2022). Examining the Effect of Organizational Trust on Individual Work Performance, Employee Treatment on Organizational Trust and Work Performance. *Research in Management and Humanities DWIJMH*, *1*(1), 111-135.

Afandi, W. N., Jamal, J., & Saad, M. Z. M. (2021). The role of CSR communication in strengthening corporate reputation. *International Journal of Modern Trends in Social Sciences*, *4*(17), 43-53.

Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536.

Alhamad, A. M., Aljanabi, B. R. H., & Almaali, A. A. H. (2022). The Relationship between Organizational Justice, Organizational Trust, and Organizational Citizenship Behavior: A Case Study of the Employees of the Karabuk University. *Sumerianz Journal of Business Management and Marketing*, *5*(1), 1-7.

AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. *International Journal of Advanced Computer Science and Applications*, *14*(2), 801-809.

Ali, A., Zulfiqar, N., Usama, M., & Ikraam, R. M. (2025). Impact of Cyber security Measures on Risk Mitigation, with the Mediating Role of Data Protection. Indus Journal of Social Sciences, 3(1), 356–372. https://doi.org/10.59075/ijss.v3i1.659

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. *Information Security Journal: A Global Perspective*, *30*(4), 189-204.

Amalia, M. P. N., & Safitri, H. (2025). The Influence of ESG Disclosure, Green Investment, and Green Fund on Company Value in the Energy Sector Listed on the Indonesia Stock Exchange. *Journal of Advanced Research in Economics and Administrative Sciences*, *6(3)*, 1-11.

Aminu, M. A. (2024). Effect of Cyber Security Measures on Financial Performance in Listed Food and Beverage Companies in Nigeria. ANUK College of Private Sector Accounting Journal, 1(2), 232-242.

Aruoren, E. E., & Tarurhor, E. M. (2023). Influence of authentic leadership on organizational trust: The mediatory role of organizational commitment. *International Journal of Management & Entrepreneurship Research*, *5*(1), 18-32.

Basri, W. S. (2023). Artificial Intelligence, Cyber Security Measures and SME's E-Operational Efficiency: Moderating Role of Employees Perception of AI Usefulness. Operational Research in Engineering Sciences: Theory and Applications, 6(4). Retrieved from http://oresta.org/menu-script/index.php/oresta/article/view/684

Baumgartner, K. T., Ernst, C. A., & Fischer, T. M. (2020). How corporate reputation disclosures affect stakeholders' behavioral intentions: mediating mechanisms of perceived organizational performance and corporate reputation. *Journal of Business Ethics*, 1-29.

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. Sustainability, 13(24), 13761. https://doi.org/10.3390/su132413761

Caviggioli, F., Lamberti, L., Landoni, P., & Meola, P. (2020). Technology adoption news and corporate reputation: Sentiment analysis about the introduction of Bitcoin. *Journal of Product & Brand Management*, *29*(7), 877-897.

Chen, Z., Mao, H., Tu, T., & Wang, H. (2024). The asymmetric effect of corporate reputation communication on flagship and non-flagship product evaluations. *Psychology & Marketing*, 1-13.

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences (2nd ed.). Lawrence Erlbaum Associates.

Dalati, S., Raudeliūnienė, J., & Davidavičienė, V. (2017). Sustainable leadership, organizational trust on job satisfaction: empirical evidence from higher education institutions in Syria. Business, Management and Economics Engineering, 15(1), 14-27.

Durst, S., Hinteregger, C., & Zieba, M. (2023). The effect of environmental turbulence on cyber security risk management and organizational resilience. Computers & Security, 137, 103591. https://doi.org/10.1016/j.cose.2023.103591

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. Behavior Research Methods, 41, 1149-1160.

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. Behavior Research Methods, 39, 175-191.

Feldman, P. M., Bahamonde, R. A., & Velasquez Bellido, I. (2014). A new approach for measuring corporate reputation. *Revista de Administraçao de empresas, 54,* 53-66.

Field, A. (2018). Discovering statistics using IBM SPSS statistics (Fifth edition). SAGE Publications.

Fombrun, C. J. (1996). *Reputation: Realizing Value from the Corporate Image*. Harvard Business School Press.

Franke, G. and Sarstedt, M. (2019). Heuristics versus statistics in discriminant validity testing: a comparison of four procedures. *Internet Research*. 29(3), 430–447. https://doi.org/10.1108/IntR-12-2017-0515

Gaskin, J., James, M., and Lim, J. (2019), "Master Validity Tool", AMOS Plugin. Gaskination's StatWiki.

George, D., & Mallery, P. (2016). IBM SPSS Statistics 23 Step by Step: A Simple Guide and Reference. Routledge.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis eight edition. *Cengage Learning EMEA: United Kingdom*.

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., ... & Khan, A. W. (2021). Cybersecurity standards in the context of operating system: practical aspects, analysis, and comparisons. *ACM Computing Surveys (CSUR)*, *54*(3), 1-36.

Hamidi, S. R., Ismail, M. A., Mohamed Shuhidan, S., & Abd Kadir, S. (2023). Corporate reputation in industry 4.0: A systematic literature review and bibliometric analysis. *Sage Open*, *13*(4), 1-19.

Hanif, M. I., Baloch, Z., & Baig, S. (2020). How Servant Leadership Affect the Organizational Trust with Mediating Role of Technological Innovation?. *International Review of Management and Marketing*, *10*(5), 74-84.

Howard, D. J. (2018). *Development of the cybersecurity attitudes scale and modeling cybersecurity behavior and its antecedents*. USF Tampa Graduate Theses and Dissertations, University of South Florida.

Huang, C. -C. Wang, Y. -M. Wu, T. -W. & Wang, P. -A. (2013). An Empirical Analysis of the Antecedents and Performance Consequences of Using the Moodle Platform, *International Journal of Information and Education* Technology, 3(2), 217-221.

Hussain, A., Mohamed, A., & Razali, S. (2020, March). A review on cybersecurity: Challenges & emerging threats. In *Proceedings of the 3rd International Conference on Networking, Information Systems & Security* (pp. 1-7).

IBM Corp. (2017). IBM SPSS Statistics for Windows (Version 25.0). IBM Corp. https://www.ibm.com/analytics/spss-statistics

Ikhsan, R., & Simarmata, J. (2021). SST-Servqual and customer outcomes in service industry: Mediating the rule of corporate reputation. *Management Science Letters*, *11*(2), 561-576.

Ion, L. M., Vodă, A. I., Butnaru, R. C., Butnaru, G. I., & Mircea Chirita, G. (2021). Effect of pharmaceutical companies' corporate reputation on drug prescribing intents in Romania. *Economic research-Ekonomska istraživanja*, *34*(1), 521-544.

Islam, T., Islam, R., Pitafi, A. H., Xiaobei, L., Rehmani, M., Irfan, M., & Mubarak, M. S. (2021). The impact of corporate social responsibility on customer loyalty: The mediating role of corporate reputation, customer satisfaction, and trust. *Sustainable Production and Consumption*, *25*, 123-135.

Jarrar, T. T., & Ibrahim, H. I. (2021). The Role of Perceived Stress as a Moderator on the Relationship between Organizational Trust and Work Engagement in Palestinian Ministries: An Empirical Approach. *International Journal Of Human Resource Studies*, *11*(2), 1-16.

Javed, M., Rashid, M. A., Hussain, G., & Ali, H. Y. (2019). The effects of corporate social responsibility on corporate reputation and firm financial performance: Moderating role of responsible leadership. *Corporate Social Responsibility and Environmental Management*, *27*(3), 1395-1409.

Jebril, I., Almaslmani, R., Jarah, B. A. F., Mugablehd, M. I., & Zaqeebae, N. (2023). The impact of strategic intelligence and asset management on enhancing competitive advantage: The mediating role of cybersecurity. *Uncertain Supply Chain Management*, 11 (2023), 1041–1046. https://doi.org/10.5267/j.uscm.2023.4.018.

Joo, B. K., Yoon, S. K., & Galbraith, D. (2023). The effects of organizational trust and empowering leadership on group conflict: psychological safety as a mediator. *Organization Management Journal*, *20*(1), 4-16.

Kamal, A., Ahmad, F., Falindah, S., Munir, A., Salleh, M., Saiful, M., & Saadon, I. (2022). The impact of customer satisfaction on loyalty in Jordanian banks: The mediating role of corporate reputation. *International Journal of Management*, *11*(2), 70-80.

Karaman, M. (2023). Keşfedici ve Doğrulayıcı Faktör Analizi: Kavramsal Bir Çalışma. *Uluslararası İktisadi ve İdari Bilimler Dergisi*, *9*(1), 47-63.

Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). *Understanding Cybersecurity Management in FinTech*. Springer International Publishing.

Kebede, A. Y., Ali, A. C., & Moges, M. A. (2022). Examining journalists organizational trust pursuant to predictive variables in the Ethiopian media industry: The case study of Amhara Media Corporation. *Cogent Social Sciences*, *8*(1), 1-17.

Kim, M. J. (2020). The effect of corporate social responsibility activities on organizational trust and job performance. *International Journal of Advanced Culture Technology*, *8*(3), 114-122.

Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. *Journal of Business Strategy*, *43*(1), 28-36.

Lam, L. W. (2012). Impact of competitiveness on salespeople's commitment and performance. Journal of Business Research, 65(9), 1328-1334

Lambert, E. G., Elechi, O. O., Baker, D., Jenkins, M., Otu, S., & Lanterman, J. L. (2022). Do the effects of organizational trust on correctional staff job attitudes vary by culture: A preliminary test with Nigerian prison staff. *Journal of Ethnicity in criminal JusticE*, *20*(1), 22-47.

Lambert, E. G., Liu, J., Solinas-Saunders, M., Wareham, J., Jiang, S., & Zhang, J. (2024). Organizational trust and work attitudes among Chinese prison officers. *Psychiatry, Psychology and Law*, 1-19.

Lee, L., & Hur, W. M. (2024). How does corporate hypocrisy undermine corporate reputation? The roles of corporate trust, affective commitment and CSR perception. *Journal of Product & Brand Management*.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734.

National Institute of Standards and Technology (2018). Framework for improving critical infrastructure cybersecurity. *URL: htstps://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, *4162018*(7).

Noor Arzahan, I. S., Ismail, Z., Yasin, S. M., & Azhar, Z. I. (2024). An exploratory factor analysis of factors affecting safety performance in Malaysian paramedic training institutes. *Journal of Academia*, *12*, 10-18.

Nuseir, M.T., Alquqa, E.K., Al Shraah, A., Alshurideh, M.T., Al Kurdi, B., Alzoubi, H.M. (2024). Impact of Cyber Security Strategy and Integrated Strategy on E-Logistics Performance: An Empirical Evidence from the UAE Petroleum Industry. In: Alzoubi , H.M., Alshurideh, M.T., Ghazal, T.M. (eds) Cyber Security Impact on Digitalization and Business Intelligence. Studies in Big Data, vol 117. Springer, Cham. https://doi.org/10.1007/978-3-031-31801-6_6

Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & management*, *58*(7), 103507.

Olaniyi, O. O., Asonze, C. U., Olabanji, S. O., & Adigwe, C. S. (2023). A regressional study on the impact of organizational security culture and transformational leadership on social engineering awareness among bank employees: The interplay of security education and behavioral change. *Asian Journal of Economics, Business and Accounting*, *23*(23), 128-143.

PCI Security Standards Council. (2018). *Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures, Version 3.2.1*.

Pérez-Cornejo, C., de Quevedo-Puente, E., & Delgado-García, J. B. (2023). The role of national culture as a lens for stakeholder evaluation of corporate social performance and its effect on corporate reputation. *BRQ Business Research Quarterly*, *26*(4), 282-296.

Pérez-Cornejo, C., de Quevedo-Puente, E., & Delgado-García, J. B. (2019). Reporting as a booster of the corporate social performance effect on corporate reputation. *Corporate Social Responsibility and Environmental Management*, *27*(3), 1252-1263.

Potgieter, A., & Doubell, M. (2020). The Influence of Employer branding and Employees' personal branding on Corporate Branding and Corporate Reputation. *African Journal of Business & Economic Research*, *15*(2), 107-133.

Pranitasari, D. (2020). The influence of effective leadership and organizational trust to teacher's work motivation and organizational commitment. *Media Ekonomi dan Manajemen*, *35*(1), 75-91.

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change*, *170*, 120872.

Ramish, M. S., Ansari, J., Saraih, U. N., Suanda, J., & Ahmed, S. (2024). Linking Corporate Trust, Corporate Image, and Customer Loyalty: The Mediating Role of Perceived Deception. *International Journal of Management Studies*, *31*(2), 469-498.

Sadq, Z. M., Ahmad, B. S., Saeed, V. S., Othman, B., & Mohammed, H. O. (2020). The relationship between intellectual capital and organizational trust and its impact on achieving the requirements of entrepreneurship strategy (The case of Korek Telecom Company, Iraq). *International Journal of Advanced Science and Technology*, *29*(2), 2639-2653.

Schumacker, R. E., & Lomax, R. G. (2010). A Beginner's Guide to Structural Equation Modeling (3th ed.). Routledge.

Silva, P., Moreira, A. C., & Mota, J. (2023). Employees' perception of corporate social responsibility and performance: the mediating roles of job satisfaction, organizational commitment and organizational trust. *Journal of Strategy and Management*, *16*(1), 92-111.

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia Computer Science*, *192*, 20-28.

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), 417-432.

Tan, L., Ting, Z., & Zheng, H. (2021, July). The effect of organizational justice on knowledge workers' job crafting——A chain mediation model of psychological ownership and organizational trust. In *Proceedings of the 2021 12th International Conference on E-business, Management and Economics* (pp. 522-527).

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

Widanti, P. P., & Sunaryo, S. (2022). Job Demands-job Resources and Organizational Trust: Mediation Role of Employee Engagement, Psychological Well-being, and Transformational Leadership. *Int. J. Econ. Bus. Manag. Res*, *6*, 52-75.

Zanabazar, A., Jigjiddor, S., & Jambal, T. (2022). The impact of work-related stress on job satisfaction and organizational trust during COVID-19 pandemic. In *SHS web of Conferences* (Vol. 135, p. 01019). EDP Sciences, 1-7.

Zeesahn, M., Qureshi, T. W., Bashir, S., & Ahmed, U. (2020). Transformational Leadership and Corporate Reputation: Mediation Effects of Employer Branding. *Journal of Management and Research*, *7*(1), 184-211.

Araştırma Makalesi

The Relationship Between Cybersecurity, Corporate Trust and Corporate Reputation in Businesses

İşletmelerde Siber Güvenlik, Kurumsal Güven ve Kurumsal İtibar Arasındaki İlişki

Polathan KÜSBECİ	**Mehmet Fatih BURAK**
Asist. Prof. Dr. Istanbul Nişantaşı University	Dr., Istanbul Beykent University
Management Information Systems	Institute of Graduate Studies
scholar@polathan.com	m.fatih@msn.com
https://orcid.org/0000-0002-4858-3853	https://orcid.org/0000-0002-9187-6491

Genişletilmiş Özet

Siber güvenlik açısından gerekli önlemlerin alınması hem kurumsal itibarın korunmasında hem de çalışanlar arasında güven oluşturulmasında önemli bir etkendir. Bu nedenle siber güvenlik uygulamaları kurumsal itibarın sağlanmasında ve örgütsel güvenin güçlendirilmesinde birbirini tamamlayan stratejik unsurlar olarak öne çıkmaktadır. Bu çalışma, literatürde daha önce incelenmemiş olan siber güvenlik, kurumsal güven ve kurumsal itibar arasındaki ilişkiyi incelemeyi amaçlamaktadır.

Siber güvenlik, kurumsal güven ve kurumsal itibar arasındaki ilişkinin incelendiği bu çalışmada, analiz için uygun bulunan 252 katılımcının anket verileri üzerinde SPSS ve AMOS programları kullanılarak bazı tanımlayıcı istatistikler, faktör analizleri, güvenilirlik ve geçerlilik analizleri, basit doğrusal regresyon analizleri ve korelasyon analizleri yapılmıştır.

Verilerin toplanmasında anket yöntemi kullanılmış olup 5'li Likert tipi ölçek tercih edilmiştir. Elde edilen veriler SPSS programı ile detaylı bir şekilde analiz edilmiştir. Bu çalışmada siber güvenliği ölçmek için Howard (2018) tarafından geliştirilen 11 maddelik bir ölçek kullanılmıştır. Siber güvenlik soruları "CSecurity" olarak kodlanmıştır. Kurumsal güveni değerlendirmek için Dalati, Raudeliūnienė ve Davidavičienė (2017) tarafından yükseköğretim kurumlarında kullanılan 6 maddeden oluşan bir ölçek kullanıldı. Bu ölçek, çalışanların kurumlarına olan güvenini ölçmeyi amaçlamaktadır ve araştırmamızda veri toplama aracı olarak uygulanmıştır. Kurumsal güven soruları "CTrust" olarak kodlanmıştır. Ayrıca Feldman, Bahamonde ve Velasquez Bellido (2014) tarafından geliştirilen 8 maddeden oluşan bir ölçek, kurumsal itibar düzeyini belirlemek için kullanılmıştır. Bu ölçek, kurumsal itibarı çok boyutlu bir şekilde ele alarak katılımcıların kurumlar hakkındaki genel algılarını ölçmeyi amaçlamaktadır. Kurumsal itibar soruları "CReputation" olarak kodlanmıştır.

Araştırmanın hipotezleri şu şekildedir; Siber güvenliğin kurumsal güven üzerinde olumlu ve anlamlı bir etkisi vardır. Siber güvenliğin kurumsal itibar üzerinde olumlu ve anlamlı bir etkisi vardır. Kurumsal güvenin kurumsal itibar üzerinde olumlu ve anlamlı bir etkisi vardır.

Regresyon analizi sonuçlarına göre siber güvenliğin kurumsal güvene doğrudan ve pozitif bir etkisi olduğu görülmektedir. Birbağımlı ve bir bağımsız değişkenin ele alındığı basit doğrusal regresyon analizinde anlamlılık düzeyi Sig.= .000 olarak belirlenmiştir. Bu sonuç iki değişken arasında istatistiksel olarak anlamlı bir ilişki olduğunu ve analizin geçerli olduğunu göstermektedir. Ayrıca F testi değerinin 1'in üzerinde olması modelin istatistiksel olarak anlamlı olduğunu desteklemektedir. Değişkenler arasındaki ilişki düzeyini gösteren R katsayısı ise .446 olarak bulunmuş olup iki değişken arasında güçlü bir ilişki olduğunu göstermektedir. Belirleme katsayısı (R^2) ise .199 olarak bulunmuş olup bağımsız değişkenin bağımlı değişkendeki toplam değişimin %19,9'unu açıkladığı anlaşılmıştır. Bağımsız değişkenin etkisi pozitif olup siber güvenliğin kurumsal güvene etkisi %22,7'dir (B= .227).

Regresyon analizi sonuçları incelendiğinde siber güvenlik faktörünün kurumsal itibar üzerinde doğrudan ve pozitif bir etkiye sahip olduğu görülmektedir. Bir bağımlı ve bir bağımsız değişkenin incelendiği basit doğrusal regresyon modelinin anlamlılık değeri Sig. =,000'dir. Yani her iki değişken arasında anlamlı bir ilişki bulunmuş ve analiz geçerli olmuştur. F testi değerinin 1'den büyük olması da modelin anlamlı olduğunu göstermektedir. Değişkenler arasındaki korelasyon katsayısını gösteren R istatistiği ise ,587 olarak bulunmuştur. Bu durumda iki değişken arasında iyi bir ilişki olduğunu söyleyebiliriz. Araştırma sonuçları incelendiğinde belirleme katsayısının (R^2 =,344) olduğu görülmektedir. Yani bağımsız değişkenin bağımlı değişken üzerindeki açıklama gücü %34,4'tür. Bağımsız değişkenin bağımlı değişken üzerindeki etkisi pozitif ve siber güvenliğin kurumsal itibar üzerindeki etkisi %51,6'dır (B =,516).

Kurumsal güvenin bağımlı değişken olan kurumsal itibar üzerindeki etkisini incelemek amacıyla yapılan regresyon analizi sonucunda bu ilişkinin istatistiksel olarak anlamlı olduğu belirlenmiştir. Hipotez testleri basit doğrusal regresyon analiz yöntemi kullanılarak gerçekleştirilmiştir. Bir bağımlı ve bir bağımsız değişkenin değerlendirildiği bu doğrusal regresyon modelinde anlamlılık düzeyi Sig.=,000 olarak elde edilmiştir. Bu durum iki değişken arasında anlamlı bir ilişki olduğunu göstermekte ve analizin geçerliliğini ortaya koymaktadır. Ayrıca F testi değerinin 1'in üzerinde olması modelin istatistiksel olarak anlamlı ve güçlü olduğunu desteklemektedir. Değişkenler arasındaki korelasyon katsayısını ifade eden R değeri ise ,474 olarak belirlenmiş olup bu sonuç iki değişken arasında anlamlı ve pozitif bir ilişki olduğunu göstermektedir. Araştırma bulgularına göre belirleme katsayısı (R^2) ,224 olarak belirlenmiş ve bu bağlamda bağımsız değişkenin bağımlı değişken üzerindeki toplam varyansın %22,4'ünü açıkladığı anlaşılmıştır. Bağımsız değişkenin etkisi pozitif, kurumsal güvenin kurumsal itibar üzerindeki etkisi ise %81,9 (B=,819) olarak bulunmuştur.

Araştırmanın bulguları, siber güvenlik, kurumsal itibar ve kurumsal güven arasındaki ilişkileri inceleyen regresyon analizleri ve korelasyon testlerine dayanmaktadır. Sonuçlar, siber güvenliğin hem kurumsal güven (r=,446, p<,001) hem de kurumsal itibar (r=,587, p<,001) üzerinde pozitif ve anlamlı bir etkiye sahip olduğunu göstermektedir. Ayrıca, kurumsal güvenin kurumsal itibar üzerinde pozitif ve anlamlı bir etkiye sahip olduğu bulunmuştur (r=,474, p<,001).

Bu çalışma, literatürde daha önce incelenmemiş olan siber güvenlik, kurumsal güven ve kurumsal itibar arasındaki ilişkiyi incelenmiştir. Günümüzün dijitalleşmiş iş dünyasında, siber güvenlik, kurumsal güven ve kurumsal itibar birbirinden bağımsız düşünülmemekte, aksine iç içe geçmiş ve kurumların sürdürülebilir başarısı için stratejik olarak önemli hale gelmiştir. Sonuç olarak, siber güvenlik, kurumsal güven ve kurumsal itibar, çağdaş organizasyonlar için stratejik başarıya ulaşmada birbirini tamamlayan ve güçlendiren temel yapı taşlarıdır. Kurumlar için bu unsurların bütünleşik bir şekilde ele alınması, dijital tehditlere karşı etkili bir koruma sağlarken aynı zamanda güçlü bir marka değeri ve sürdürülebilir bir iç yapının inşasını da mümkün kılar. Bu nedenle, kurumların dijital dönüşüm süreçlerinde yalnızca teknolojik altyapılarını değil aynı zamanda kurumsal itibarlarını ve iç güven yapılarını da kapsayacak bütünsel bir geliştirme sürecini benimsemeleri gerekir.

Yöntem (nicel), araç (SPSS ve AMOS), örneklem, kullanılan ölçekler, analiz zamanı ve analize katılan bireylerin görüşleri bu çalışmanın sınırlılıklarını oluşturmaktadır. Gelecekteki çalışmalarda, bu araştırma farklı ülkelerde ve bölgelerde, farklı yöntem ve araçlarla tekrarlanabilir ve farklı faktörler eklenerek farklı etkilerle analiz edilebilir. Gelecekteki çalışmalarda, dijital dönüşüm sürecindeki değişkenlerin siber güvenlik algıları üzerindeki etkilerinin değerlendirilmesi bu alandaki bilginin artırılmasına önemli katkı sağlayacaktır.