Innovation in Corporate Cyber Security

Mustafa Şenol
Faculty of Engineering and Architecture
Istanbul Gelisim University
Istanbul, Turkey
msenol@gelisim.edu.tr

2023 4th International Informatics and Software Engineering Conference (IISEC) | 979-8-3503-1803-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/IISEC59749.2023.10390993

***Abstract*— The invention of computers, the development of information and communication systems and technologies, along with the gains they have provided, have made the realm of information technology an indispensable part of human life. In a world that has become increasingly digitized in every aspect, the dangers and threats directed towards information, information systems, valuable assets, and the emerging power continue to grow day by day. As the importance of cybersecurity increases in every field and at every level to counter these dangers and threats, corporate cybersecurity has become an essential element of today's business world. The dangers and threats that arise in the cyber environment pose significant risks to organizations of all sizes, and traditional security measures are no longer sufficient to provide adequate protection. The necessity of "Innovation in Corporate Cybersecurity" has emerged as a process of developing a more agile, effective, and results-oriented approach to addressing cyber threats and risks. This work attempts to highlight the foundations, importance, innovative technologies and approaches, implementation, challenges, and risks of innovation in corporate cybersecurity, as well as the benefits it can provide to organizations, while also offering insights and predictions.**

Keywords*— *Information security, cyber security, corporate cyber security, cyber security management system, innovation.

I. INTRODUCTION

From humanity's past to the present, the power and significance of knowledge have grown, and the era we currently live in is referred to as the "information age." With the invention of computers, the development of digital information and communication systems, and their becoming essential parts of human life, the information age is also known as the "digital age." However, dangers and threats directed towards information and the power it provides continue to increase every day.

The quote by futurist Toffler, "Our technological powers increase, but the side effects and potential hazards also escalate." [1] reflects current reality. The concept of "information security," born out of the need to protect information, has become integrated with the concept of "cybersecurity" today, encompassing individuals, institutions, and states at every level, with a focus on securing information systems and technologies (IT).

As technology advances and the cyber space composed of information communication systems and networks is increasingly utilized, the effectiveness of information and the power it provides have grown, adding indispensable additional value to the lives of individuals, institutions, and nations.

Within the trio of "Individual - Organization - State/Nation," organizations and institutions are one of the fundamental components that make up the individuals, i.e., employees, and the states. As the digital age rapidly progresses, the importance of national cybersecurity within national security has increased, and the security of cyber environments, including valuable information assets of institutions, namely corporate cybersecurity, has become an indispensable element of today's business world. Establishing and operating effective information security / cybersecurity management systems for institutions has become critically important.

Technological advancements have simplified business processes, but at the same time, they have made cyber threats more complex and widespread. As the types, severity, and complexity of cyber threats and attacks increase, their detection has become more challenging, while the technical knowledge, training, and education levels of cyber attackers have decreased. [2] The dangers and threats that arise in the cyber environment pose significant risks to organizations of all sizes, and traditional security measures are no longer sufficient to provide adequate protection. This is where the concept and necessity of "Innovation in Corporate Cybersecurity" come into play.

Innovation in corporate cybersecurity is a process of developing a more agile, effective, and results-oriented approach to counter cyber threats and risks. It enables institutions to prepare their security strategies and policies not only against existing and known threats but also against potential future threats. While traditional security approaches focus on known and specific threat types, innovation is designed to understand the variable nature of threats and respond to them more rapidly and intelligently.

In parallel with developments in the cyber domain and the increasing threats and risks, the need and importance of cybersecurity have been recognized. However, there are shortcomings and deficiencies, particularly in terms of the adequacy and currency (i.e., innovation) of measures taken in corporate cybersecurity. This study aims to elucidate why innovation in corporate cybersecurity is critically important, how it can be implemented, what benefits it can provide to organizations, and how success can be achieved, based on these thoughts and observations. When the role of innovation in cybersecurity is understood, the importance of shaping a safer digital future for institutions will also become better understood.

In this context, the foundations of corporate cybersecurity and innovation are explained, innovative technologies and approaches in corporate cybersecurity are examined, a focus is placed on best practices for achieving corporate cybersecurity innovation and the challenges and risks of cybersecurity innovation are evaluated. Additionally, future predictions regarding corporate cybersecurity innovation are provided, offering insights and recommendations for organizations, institutions, businesses, and researchers working in this field at all levels.

979-8-3503-1803-6/23/$31.00 ©2023 IEEE

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on January 08,2025 at 08:13:16 UTC from IEEE Xplore. Restrictions apply.

II. Foundations of corporate Cyber security And Innovation

With the advancement of technology, the development of computers, information systems, and networks, we have entered the age of information, where nearly all data and information exist in digital format. Alongside the cyber environment created by information systems and networks, many terms and concepts related to the digital realm have entered human life, often beginning with the prefix "cyber." One of the most common terms among these is "cybersecurity," which encompasses "information security," covering the security of data and information, and is considered a broader concept with strategy documents published. [3]

The effective provision of cybersecurity requires the correct use of terms and a common understanding, primarily to achieve the goals set by strategies and policies. The implementation of the established strategies and policies, the efficient operation of the systems, and their timely updates and changes, in short, their "innovation," are of great importance.

A. Cybersecurity

Numerous studies have been conducted on information security and, consequently, there are many definitions in the literature. In the 2020-2023 National Cybersecurity Strategy and Action Plan of Turkey, the definition of "information security" is given as "All activities conducted to prevent unauthorized use, access, disclose, erasion, change and harm of/on information technologies and information, and ensure that those systems and information are available to authorized persons and processes when necessary and with required quality." [4].

When it comes to personal cybersecurity, individuals typically think of the security of their online accounts, credit cards, and the security of their computers, smart devices, and objects. However, when approached from a corporate perspective, much broader meanings and requirements emerge, and the national cybersecurity dimension extends to encompass all citizens and institutions of a country, even reaching international dimensions. With this broad and unlimited perspective, the definition of "cybersecurity" is given as "All activities that involves protecting the information technologies which constitutes the cyberspace from attacks, ensuring the confidentiality, integrity and availability of those systems, detecting attacks and cyber incidents, activating response mechanisms against those, and restoring the systems back to pre-cyber incident conditions." [4].

B. Corporate Cybersecurity

Cybersecurity efforts typically begin at the government level under the umbrella of national security and extend down to the individual level, employing various methods, tools, and objectives. Within this framework, corporate cybersecurity, situated between the government and individual levels, forms the backbone of cybersecurity efforts [5].

When viewed from a corporate perspective, considering the above description summarizing the measures to be taken and the actions to be carried out for ensuring cybersecurity, an organization's cybersecurity duties and responsibilities will also be clearly outlined as follows:

- Protecting the information systems constituting the organization's cyber space from attacks,
- Ensuring the confidentiality, integrity, and availability of data and information processed in the organization's cyber environment,
- Detecting cyberattacks and cyber incidents targeting the organization's IT systems,
- Activating response mechanisms against cyber incidents and attacks on the organization's IT assets,
- Restoring the systems to their pre-cybersecurity incident state following cyber incidents and attacks targeting the organization.

To fulfill these duties and responsibilities, it is of great importance to establish a corporate cybersecurity management system and operate this system effectively. This system is vital for protecting not only the information assets of the organization but also its reputation, legal obligations, employees, and other tangible and intangible assets. In this context, following internationally recognized standards, such as ISO/IEC 27001 (Information security, cybersecurity, and privacy protection - Information security management systems - Requirements) and COBIT (Control Objectives for Information and Related Technologies), is essential, as these standards promote best practices and approaches that benefit organizations in various aspects, often being mandatory in the public sector.

C. Innovation

Innovation, as defined in dictionaries, includes "the use of new methods in social, cultural, and managerial contexts to adapt to changing conditions" [6] and "the creation of a new way of doing something, whether concrete or abstract" [7]. It involves a process that encompasses the adoption of new ideas or behaviors within an organization, generating ideas for new products and processes, developing technology, managing production and marketing activities, and converting knowledge into economic and social benefit [8].

Innovation is a conscious and systematic process that involves a strategic perspective, not merely chasing the new and innovative but also improving, enhancing, and differentiating the existing. [9] It is the process of creating, developing, implementing, and generating value from new ideas, products, services, or processes.

Innovation aims to improve the current state, increase efficiency, gain a competitive advantage, expand the market, ensure sustainability, create new opportunities, and build a better future. Innovation can affect various fields, including the business world, technology, science, art, education, and many others, and it can occur in various forms. It is not limited to just developing new products or technologies but also encompasses efforts to enhance business processes, business models, marketing, design, corporate structures, and service delivery, among many other areas.

With the advancement of technology, the type, intensity, and complexity of cyber threats and attacks are increasing, making their detection and prevention more difficult. Traditional security measures are no longer sufficient to provide adequate protection against new dangers and threats emerging in the cyber environment,

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on January 08,2025 at 08:13:16 UTC from IEEE Xplore. Restrictions apply.

which pose significant risks to organizations. In this context, innovation in cybersecurity can play a crucial role by anticipating new threat types, securely storing data, swiftly addressing security vulnerabilities, and enhancing organizations' resilience against cyberattacks. Therefore, there is a need for greater awareness and prioritization of cybersecurity in the corporate world, with a focus on incorporating innovation into security strategies and policies.

In a period when cyber threats and attacks are increasing in complexity and severity alongside technological advancements, it is inevitable for organizations to review their approaches to cybersecurity and embrace innovative thinking. Innovation stands out as a crucial key to staying ahead of cyber threats and strengthening the protection of information assets.

III. Innovative Technologies, Approaches, and Best Practices In Corporate Cybersecurity

A. Innovative Technologies and Approaches in Corporate Cybersecurity

In a rapidly changing landscape where cyber threats are evolving rapidly and attacks are becoming more sophisticated, cybersecurity is gaining increasing importance. It necessitates organizations to constantly review and renew their security strategies. In the corporate world, cybersecurity is an area that constantly requires innovation to cope with the ever-growing complexity of cyber threats and attacks. Adapting digital technologies for innovative opportunities and creating value-added services and processes in line with information systems and technologies is a top priority for corporate digital transformation [10]. Innovative technologies and approaches can strengthen corporate cybersecurity defenses and better prepare organizations against potential threats.

There is a wide range of innovative technologies and approaches that can be used for rejuvenation in cybersecurity. Some innovative technologies and approaches that can be used in corporate cybersecurity and should be taken into consideration in this field are presented in "Table I." These can assist organizations in being more effective in cybersecurity and better prepared against cyber threats.

TABLE I. Technologies and Approaches for Innovation in Corporate Cybersecurity

R. Nu.	Technologies and Approaches for Innovation in Corporate Cybersecurity
1.	Data Analytics and Business Intelligence
2.	Cloud Computing Security
3.	Internet of Things (IoT) Security
4.	Blockchain Technology
5.	Virtual Private Networks and Encryption Technologies
6.	Identity and Access Management
7.	Machine Learning and Artificial Intelligence
8.	Behavioral Analysis and Insider Threat Detection
9.	Zero Trust Model
10	Historical Analysis and Threat Intelligence
11.	Attack Simulation
12.	Security Automation - Regulation and Incident Response
13.	Cybersecurity Training and Awareness

- Data analytics and business intelligence assist organizations in identifying abnormal behaviors by analyzing large datasets. This technology provides a better understanding of security incidents and threats and facilitates the rapid assessment of events. Monitoring trends in incidents, especially, helps in identifying security vulnerabilities more quickly.
- Cloud computing security ensures the safety of data and applications in cloud infrastructure. Cloud service providers offer security controls such as encryption, robust authentication, and access monitoring. When working with cloud-based services, organizations should adopt these security measures.
- Internet of Things (IoT) security ensures the security of IoT devices. These devices collect and share data through sensors and connections. IoT security includes measures such as encryption, authentication, and updates for the security of these devices.
- Blockchain is used to enhance data security and integrity. This technology, created by chaining blocks together, makes data modification difficult and provides a reliable audit trail.
- Virtual Private Networks (VPNs) and robust encryption technologies enable secure data transmission and storage. VPNs use encryption to securely transmit data over the internet, while encryption technologies protect data during storage or transmission.
- Identity and Access Management are used to ensure the right people have the right access. This technology verifies users' identities, manages access policies, and monitors access.
- Machine learning and artificial intelligence are used to detect cyber threats, monitor abnormal behaviors, and provide automated responses. These technologies can quickly adapt to evolving threats and offer continuous learning capabilities.
- Behavioral analysis recognizes normal behaviors of users and systems and detects abnormal activities. Insider threat detection monitors and prevents potential threats within the organization.
- The Zero Trust model is based on the principle of not trusting any device or user by default. The identity of every user and device is continuously verified, and access privileges are minimized.
- Historical analysis prepares for future threats by examining past cyberattacks. Threat intelligence provides information about current threat data and attack trends.
- Attack simulation allows organizations to simulate attack scenarios and identify vulnerabilities, thus improving defense measures.
- Security automation is used to quickly detect and respond to security incidents, reducing human errors and speeding up response processes.
- Educating and raising awareness among employees and users about cyber threats enhances

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on January 08,2025 at 08:13:16 UTC from IEEE Xplore. Restrictions apply.

organizational security. Training creates better awareness of secure behaviors and threats.

These technologies and approaches can help organizations be more effective in cybersecurity and better prepared for cyber threats. However, the needs, capabilities, and opportunities of each organization vary. Therefore, selecting and using the right technology and approaches will depend on each organization's specific requirements and capabilities.

B. Best Practices for Corporate Cybersecurity Innovation

In today's technology-driven world, corporate cybersecurity holds vital importance for organizations. Evolving threats, data breaches, and cyberattacks compel organizations to adopt an innovative approach. Organizations must establish and operate cybersecurity management systems in line with internationally recognized standards, continually improving compliance, adequacy, and effectiveness. [11]

In this context, for innovation in corporate cybersecurity, organizations should utilize best practices that are supported by international standards, widely adopted, tested, and proven effective. Some of these best practices, as presented in "Table II," should be considered.

TABLE II. BEST PRACTICES FOR CORPORATE CYBERSECURITY INNOVATION

R. Nu.	Best Practices for Corporate Cybersecurity Innovation
1.	Developing Cybersecurity Strategies and Policies
2.	Creating a Transformation Team
3.	Allocating Budget for Transformation
4.	Cultivating a Risk-Taking Culture
5.	Defining Transformation Processes
6.	Disseminating Transformation Across the Organization
7.	Compliance and Security Awareness
8.	Being Open to Feedback and Evaluating Employee Ideas
9.	Cybersecurity Controls and Audits
10	Assessing and Improving Transformation Projects
11.	Promoting Transformation, Celebrating Achievements, and Rewarding
12.	Collaboration and Information Sharing
13.	Continuous Education and Awareness Programs

- First and foremost, the security strategies and policies of organizations should be determined, security objectives and rules should be clearly defined. These documents form the foundation of a security culture.
- A dedicated team should be established to support an innovative approach. This team is responsible for identifying security vulnerabilities, developing and implementing solutions against new threats.
- A budget should be allocated for innovative projects and security enhancements. These resources are used to evaluate, update, and support cybersecurity projects.
- A culture should be created to encourage employees to propose innovative ideas and take risks in the field of cybersecurity. However, it is essential to manage these risks effectively and closely monitor security measures.
- Innovative projects should be defined, and plans for how these projects will be executed and managed should be established. These processes enable the development and testing of new security solutions.
- Innovative solutions should not be limited to the cybersecurity team alone; efforts should be made to promote them throughout the organization to increase security awareness among all employees and encourage their contributions to security practices.
- It is important for innovative projects to meet compliance requirements and security standards. This ensures compliance with legal obligations and the protection of data and information.
- Employees' security-related ideas and feedback should be listened to and evaluated, fostering a more comprehensive approach by encouraging the workforce to participate in cybersecurity processes.
- Innovative solutions should be continuously audited, and security controls should be applied. This helps in the ongoing assessment and improvement of cybersecurity.
- Completed projects should be analyzed, their successes and weaknesses identified, and improvements should be made using these experiences for future innovative projects.
- Innovation and security achievements should be celebrated and rewarded. This boosts employee morale and recognizes their contributions to cybersecurity.
- Collaboration with other organizations and sectors should be encouraged to promote information sharing. This can help in more effective combat against new threats.
- Regular security training should be provided to employees, and security awareness programs should be organized. This helps reduce security vulnerabilities caused by the human factor.

In the rapidly evolving digital landscape, managing innovation correctly is essential to gain a competitive edge, drive business innovation, enhance customer experiences, and improve efficiency and productivity. Creating value in the strategies developed often results from high levels of digitization in new business models, effective processes, and successful innovation. [12]

IV. CHALLENGES AND RISKS OF CORPORATE CYBERSECURITY TRANSFORMATION

Due to the widespread nature of information systems and rapid technological changes, a reliable framework is required to adequately control the entire information environment and prevent unacceptable risks that may pose a threat to the organization. [12] The processes of corporate cybersecurity transformation face a series of challenges and risks. A cybersecurity management system, by implementing a risk management process, provides assurance to relevant parties that confidentiality, integrity, and accessibility, which form the foundation of cybersecurity, are adequately managed. [11] Below are some of the main challenges and risks encountered in corporate cybersecurity transformation:

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on January 08,2025 at 08:13:16 UTC from IEEE Xplore. Restrictions apply.

- Cybersecurity threats are constantly evolving. Attackers develop new methods of attack, making it challenging for security experts to keep up. Unknown threats, especially zero-day attacks, can pose significant risks to organizations.
- The use of new software or systems during the innovation process can expose security vulnerabilities. These vulnerabilities can allow cyber attackers to infiltrate the system or gain access to sensitive data.
- Innovations can violate data privacy and compliance requirements. Particularly, non-compliance with local and international laws and regulations such as the Personal Data Protection Law (KVKK - Turkey) and the European Union General Data Protection Regulation (GDPR) can result in hefty fines and reputational damage.
- When innovations are implemented incorrectly or fail to provide adequate protection, they can jeopardize business continuity. Data loss or service interruptions can hinder business operations.
- Internet of Things (IoT) devices and connected objects can introduce new security risks as they become integrated into business networks. These devices can serve as gateways for malware and cyberattacks.
- The shortage of qualified cybersecurity experts can make it difficult to carry out transformation projects and resolve security issues. Businesses may struggle to find and hire these experts.
- A lack of cybersecurity awareness among employees can amplify internal threats and user errors, making them a greater risk. Lack of training and awareness can hinder the effective implementation of security measures.
- Artificial intelligence and automation can offer significant benefits in cybersecurity. However, the incorrect configuration or misuse of these technologies can increase security risks.
- Innovation projects often result in high costs, and businesses may find it challenging to cope with budget constraints. Allocating sufficient resources for security can pose problems.
- With technology evolving rapidly, slow progress or disruptions in transformation projects can jeopardize security. Organizations may need to expedite their processes to keep up with rapidly changing threats.

To overcome these challenges and risks, thorough planning, continuous review, and updates are necessary. As organizations continue to adapt to the ever-changing technological landscape, they will need to invest more in security improvements and technological innovations to defend against attacks before breaches occur. In particular, cybersecurity awareness, training, and collaboration can help organizations navigate these challenges.

V. Future Corporate Cybersecurity Innovation

Corporate cybersecurity is constantly evolving with technological advancements, changing threat landscapes, and regulations. In the future, corporate cybersecurity renewal will become even more critical alongside evolving technologies and changing threat scenarios. Developing strategies, planning, and process improvement efforts involve looking back at the past, learning from it, assessing the current situation, and identifying new opportunities to determine the future state and guide the organization towards its set goals. [13] When preparing corporate strategies and policies, the principle of conducting cybersecurity activities based on corporate governance, continuity, and sustainability principles with gains, objectives, programs, and projects from the past to the future is adopted. [4]

Considering factors that may influence future corporate cybersecurity strategies and policies when thinking about how renewal can occur in future corporate cybersecurity, based on learning from the past and evaluating the current situation, the following factors can be taken into account:

- In the future, organizations will better understand threats and protect data more effectively by using big data analytics. New technologies and methods will be developed to comply with data privacy regulations.
- Organizations will invest more in secure cloud services and develop strategies for securing data in the cloud. Secure cloud architectures and services will be of great importance during this period.
- As the number of Internet of Things (IoT) devices increases, their security will become a bigger concern. IoT security will include defense mechanisms against new threats and the establishment of new industry standards.
- Blockchain technologies will be used to enhance data integrity and reliability. These technologies will play a significant role in the security of corporate networks and operations.
- Quantum computers could threaten traditional encryption methods. Therefore, post-quantum encryption solutions will be developed to prepare for future cybersecurity threats.
- Identity and access management will be developed and customized to meet increasingly complex business requirements. Multi-factor authentication and biometric technologies will become more widespread.
- Machine learning and artificial intelligence will be used more extensively to detect and prevent cyber threats. These technologies will enhance the ability to identify attacks, and the detection of cyberattacks will occur faster and more effectively through behavioral analysis and threat monitoring systems.
- A zero-trust model, representing an approach where nothing is considered trustworthy, will be adopted.
- Automation will be used more in cybersecurity operations, increasing the ability to respond quickly to cyberattacks.

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on January 08,2025 at 08:13:16 UTC from IEEE Xplore. Restrictions apply.

- Secure software development principles will be emphasized more, and software security will be integrated in a planned manner.
- Information technology collaboration will encourage threat intelligence sharing among different organizations. Endpoint security will gain more importance with the increasing trend of mobile work and Bring Your Own Device (BYOD).
- Organizations will increasingly update their cybersecurity capabilities, rapidly adapt to regulatory changes, and make renewal a central focus of cybersecurity strategies.
- To prevent employees from continuing to be a weak link in cybersecurity, more focus will be placed on the human factor. Providing planned and comprehensive cybersecurity training and awareness programs to employees will help prevent internal threats and social engineering attacks.
- Cybersecurity industry standards will assist organizations in following best practices and providing standardization in the international sector. Global cooperation and coordination will contribute to the development of international cybersecurity standards and solutions.

These factors will form the foundation of future corporate cybersecurity strategies. Organizations of all types and levels must develop flexible and continuously updated cybersecurity strategies and policies to adapt to these changes.

VI. Conclusion and Recommendations

In today's world, information systems and infrastructure have become indispensable to human life at personal, corporate, and national levels due to the invention of computers, the development of digital information and communication systems, and the value-added they provide. In the digitized world at every level and in every field, dangers and threats to information, information systems, valuable assets, and emerging cyberpower continue to increase day by day.

While the importance of cybersecurity is increasing within national security, ensuring the security of corporate cyber environments, institutions and organizations, has become an indispensable element of today's business world that constitutes states.

The dangers and threats arising in the cyber environment pose significant risks to organizations of all types and sizes, and traditional security measures can no longer provide adequate protection. Establishing information security / cybersecurity management systems has become critically important for organizations, and the concept and necessity of "Innovation in Corporate Cybersecurity" have emerged as a process to develop more agile, effective, and result-oriented approaches to cyber threats and risks.

Cybersecurity innovation enables organizations to prepare their security strategies and policies not only for existing and known threats but also for potential future threats that may occur at any moment and in an uncertain future. While traditional security approaches focus on known and specific threat types, cybersecurity innovation is designed to understand the variable nature of threats and respond to these threats more quickly and intelligently.

With these thoughts and findings, this study, which includes preliminary information about innovation in corporate cybersecurity, explains why it is critically important, what innovative technologies and approaches are, how they can be implemented, what challenges and risks exist, what benefits can be provided to organizations, and how they can be successful in the future.

In conclusion, as information systems and technologies continue to evolve, cyber threats and risks are also changing every day. For organizations, cybersecurity is an ongoing process. Considering technological advancements and the evolution of threats, continuous development of new approaches and strategies in cybersecurity is vital. Therefore, organizations should keep track of changes in the cyber environment and security world, invest in this field, continuously review, update, and improve their security strategies and policies to become more resilient to potential future threats and risks.

This study, which includes preliminary information about renewal in corporate cybersecurity, can serve as a small guide to make the efforts and research of organization managers and relevant employees in this regard more effective. By embracing the ideas and recommendations in this study, organizations can strengthen their cybersecurity and become more resilient to future threats and risks. Given the complexity and ubiquity of cyber threats, I hope that academic groups and researchers will focus on this issue, and their views and suggestions will contribute to the development of more resilient solutions in the future.

References

[1] Goodman, M., “Future Crimes”, Corgi Books, GB, 2016.

[2] ITU, Global Cybersecurity Agenda High-Level Experts Group Global Strategic Report. ITU Press, Switzerland, 2008.

[3] Bozgeyik, A., “Corporate Cyber Security Management”, Adalet Publ., Ankara, 2021.

[4] T.R. Ministry of Transport and Infrastructure, “National Cyber Security Strategy and Action Plan (2020-2023)”, Ankara, 2020.

[5] Kahraman, M. et al., “Institutional Cybersecurity from Military Perspective”, International Journal of Information Security Science, Vol.5 No 1, Ankara, 2016.

[6] TDK Dictionary, https://sozluk.gov.tr/ (Accessed: 15 August 2023).

[7] The Britannica, https://www.britannica.com/topic/innovation-creativity, (Accessed: 15 August 2023).

[8] Uzkurt, C., “What is Innovation and What is It Not?” (Technology, Innovation and Entrepreneurship, Ed.: Uzkurt, C. and Önder, G.), Anadolu Univ. Publ., Eskisehir, 2020.

[9] Elçi, Ş., “Innovation Guide: A Handbook of Profitability and Competition”, (A Journey to the World of Innovation, Ed.: Karaata, S.), EGIAD Publ., Izmir, 2012.

[10] TUBITAK BILGEM, “Information Technologies Management Guide”, TUBITAK Publ., Izmit, 2021.

[11] ISO/IEC, “ISO/IEC 27001 Information security, cybersecurity and privacy protection – Information security management systems - Requirements”, ISO/IEC Publ., Switzerland, 2022.

[12] ISACA, “COBIT® 2019 Framework: Introduction and Methodology”, ISACA Pub., USA, 2018.

[13] Knerler, K. et al., “11 Strategies of a World Class Cybersecurity Operations Center” MITRE Pub., USA, 2022.

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on January 08,2025 at 08:13:16 UTC from IEEE Xplore. Restrictions apply.