Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

GU J Sci, Part C, 11(4): 1116-1130 (2023)

Measurement of the Cybersecurity Strategy Effectiveness with a Scorecard Based on Risk Analysis

Özlem EVRE[1*], Bünyamin CİYLAN[2]

[1] Gazi University, Computer Forensics, Graduate School of Informatics, Ankara, Turkey

[2] Gazi University, Department of Computer Engineering, Technology Faculty, Ankara, Turkey

Article Info

Research article
Received: 18/08/2023
Revision: 13/11/2023
Accepted: 30/11/2023

Keywords

National Cybersecurity Strategy
Effectiveness of Strategy
Strategy Implementation Model
Scorecard for Cybersecurity Strategy
Measuring Cybersecurity Strategy

Makale Bilgisi

Araştırma makalesi
Başvuru: 18/08/2023
Düzeltme: 13/11/2023
Kabul: 30/11/2023

Anahtar Kelimeler

Ulusal Siber Güvenlik Stratejisi
Stratejinin Etkinliği
Strateji Uygulama Modeli
Siber Güvenlik Stratejisi Puan Kartı
Siber Güvenlik Stratejisini Ölçme

Graphical/Tabular Abstract (Grafik Özet)

In this article, it is mentioned that a strategy model was prepared in order to eliminate the lack of strategy implementation, which is a global problem, and the prepared action plan was evaluated using the scorecard. A risk-based scorecard was created to develop an effective strategy and ensure its continuity. / Bu makalede küresel bir sorun olan strateji uygulama eksikliğinin giderilmesi amacıyla bir strateji modelinin hazırlandığı ve hazırlanan eylem planının puan kartı kullanılarak değerlendirildiğinden bahsedilmektedir. Etkin bir strateji geliştirmek ve sürekliliğini sağlamak amacıyla risk bazlı puan kartı oluşturulmuştur.

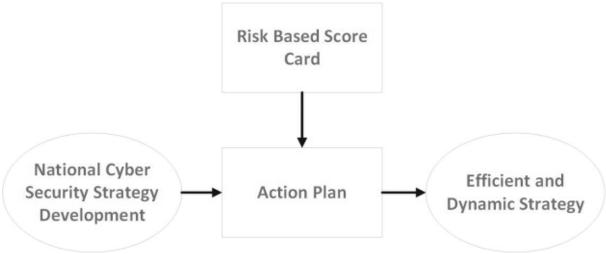

Risk Based Score Card
National Cyber Security Strategy Development
Action Plan
Efficient and Dynamic Strategy

***Figure A**: Effective Strategy Development /**Şekil A:** Etkili Strateji Geliştirme*

Highlights (Önemli noktalar)

- *To create a living and self-renewing Information Security Ecosystem / Yaşayan ve kendini yenileyen bir Bilgi Güvenliği Ekosistemi oluşturmak.*
- *Increasing the effectiveness of the strategy / Stratejinin etkinliğini arttırmak*
- *Guiding the creation of a new strategy / Yeni bir strateji oluşturulmasına yol göstermek*

Aim (Amaç): *The aim is to emphasize that sustainability and continuous improvement will be increased by using the scorecard based on risk analysis by implementing the proposed action plan through the strategy model. / Önerilen eylem planının strateji modeli üzerinden hayata geçirilmesiyle risk analizine dayalı puan kartı kullanılarak sürdürülebilirliğin ve sürekli iyileştirmenin artırılacağının vurgulanması amaçlanmaktadır.*

Originality (Özgünlük): *This study suggests that measurement as a method of increasing productivity, which has not been discussed much until now, may be the solution. / Bu çalışma, bugüne kadar çok fazla tartışılmayan bir verimlilik artırma yöntemi olarak ölçümün çözüm olabileceğini öne sürüyor.*

Results (Bulgular): *Thanks to the scorecard, which will shed light on the extent to which the action plan headings have been fulfilled and will also provide information about auditing and reporting, which is the last stage of the strategy implementation model, the aspects of the strategies that are not working and the actions that need to be added or improved will be quickly revealed. / Eylem planı başlıklarının ne ölçüde yerine getirildiği konusunda ışık tutacak, aynı zamanda strateji uygulama modelinin son aşaması olan denetim ve raporlama konusunda da bilgi verecek olan puan kartı, sayesinde stratejilerin çalışmayan yönleri, eklenmesi veya geliştirilmesi gereken aksiyonlar hızla ortaya çıkacaktır.*

Conclusion (Sonuç): *While developing a national cybersecurity strategy or updating the existing strategy, attention should be paid to ensure that the strategy is effective, constantly evolving, and reinforcing weak points. A successful strategy must be fed with feedback, measured, and continuously improved. / Ulusal siber güvenlik stratejisi geliştirirken veya mevcut stratejiyi güncellerken stratejinin etkili olmasına, sürekli gelişmesine ve zayıf noktaları güçlendirmesine dikkat edilmelidir. Başarılı bir stratejinin geri bildirimlerle beslenmesi, ölçülmesi ve sürekli iyileştirilmesi gerekir.*

*Corresponding author, e-mail: ozlem.evre@gazi.edu.tr

DOI: 10.29109/gujsc.1345984

Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

http://dergipark.gov.tr/gujsc

Measurement of the Cybersecurity Strategy Effectiveness with a Scorecard Based on Risk Analysis

Özlem EVRE[1*], Bünyamin CİYLAN[2]

[1] *Gazi University, Computer Forensics, Graduate School of Informatics, Ankara, Turkey*

[2] *Gazi University, Department of Computer Engineering, Technology Faculty, Ankara, Turkey*

Article Info

Research article
Received: 18/08/2023
Revision: 13/11/2023
Accepted: 30/11/2023

Keywords

National Cybersecurity Strategy
Effectiveness of Strategy
Strategy Implementation Model
Scorecard for Cybersecurity Strategy
Measuring Cybersecurity Strategy

Abstract

Although the rapid acceleration of technology offers solutions that will make human life easier, it also brings technological threats that will negatively affect human life and cause serious problems. Attacks, thefts, and espionage using technology increase exponentially yearly compared to the previous. To eliminate this problem that affects the whole world, many countries prioritize creating cybersecurity strategies to protect their information and resources and develop effective implementation methods. Despite the abundant literature, there is a significant gap in the effective implementation of strategies. While evaluating the strategy, measurement is made regardless of the risks arising if the action plan is not fulfilled. For this reason, it is recommended to assess the risk that will occur if the action titles are not implemented to eliminate this shortcoming. The aim is to emphasize that sustainability and continuous improvement will be increased by using the scorecard based on risk analysis by implementing the proposed action plan through the strategy model. The use of scorecards to overcome the increasing challenges arising from digital transformation today will contribute to evaluating the strategy, eliminating its shortcomings, and providing self-assessment. This study suggests that measuring as a method of increasing efficiency, which has not been discussed much until now, may be the solution. To ensure the security of the smart world, there is a need for a sustainable and effective strategy that can keep up with digital realities, renewing itself.

Siber Güvenlik Stratejisi Etkinliğinin Risk Analizine Dayalı Skor Kart ile Ölçülmesi

Makale Bilgisi

Araştırma makalesi
Başvuru: 18/08/2023
Düzeltme: 13/11/2023
Kabul: 30/11/2023

Anahtar Kelimeler

Ulusal Siber Güvenlik Stratejisi
Stratejinin Etkinliği
Strateji Uygulama Modeli
Siber Güvenlik Stratejisi Puan Kartı
Siber Güvenlik Stratejisini Ölçme

Öz

Teknolojinin hızla ivmelenmesi insan hayatını kolaylaştıracak çözümler sunsa da insan hayatını olumsuz etkileyecek ve ciddi sorunlara yol açacak teknolojik tehditleri de beraberinde getiriyor. Teknolojiyi kullanan saldırılar, hırsızlıklar ve casusluk olayları her yıl öncekine göre katlanarak artıyor. Tüm dünyayı etkileyen bu sorunu ortadan kaldırmak için birçok ülke, bilgi ve kaynaklarını korumaya yönelik siber güvenlik stratejileri oluşturmaya ve etkili uygulama yöntemleri geliştirmeye öncelik veriyor. Literatürün bolluğuna rağmen stratejilerin etkili bir şekilde uygulanması konusunda önemli bir boşluk bulunmaktadır. Strateji değerlendirilirken aksiyon planının yerine getirilmemesi durumunda ortaya çıkacak risklere bakılmaksızın ölçüm yapılır. Bu nedenle bu eksikliğin giderilmesine yönelik eylem başlıklarının hayata geçirilmemesi durumunda oluşacak riskin değerlendirilmesi önerilmektedir. Önerilen eylem planının strateji modeli üzerinden hayata geçirilmesiyle risk analizine dayalı puan kartı kullanılarak sürdürülebilirliğin ve sürekli iyileştirmenin artırılacağının vurgulanması amaçlanmaktadır. Günümüzde dijital dönüşümün getirdiği artan zorlukların üstesinden gelmek için puan kartlarının kullanılması, stratejinin değerlendirilmesine, eksikliklerinin giderilmesine ve öz değerlendirmenin sağlanmasına katkı sağlayacaktır. Bu çalışma, bugüne kadar pek fazla tartışılmayan, verimliliği artırma yöntemi olarak ölçmenin çözüm olabileceğini öne sürüyor. Akıllı dünyanın güvenliğinin sağlanması için dijital gerçekliğe ayak uydurabilen, kendini yenileyebilen, sürdürülebilir ve etkili bir stratejiye ihtiyaç var.

1. INTRODUCTION (GİRİŞ)

Cybersecurity is the protection of digital information and its infrastructure. Cybersecurity addresses the challenges and threats of cyberspace to secure the benefits and opportunities of digital life [1]. Regarding cybersecurity and information security, it will not be enough to buy the latest

*Corresponding author, e-mail: ozlem.evre@gazi.edu.tr

DOI: 10.29109/gujsc.1345984

technology devices/systems, use anti-virus software, and update periodically. The point is that the weakest link is "human". Recent studies reveal that the greatest threat to an organization's information security is caused by careless corporate employees who deliberately or unintentionally misuse the organization's information assets [2]. Similarly, Mills et al. [3] emphasized in their study that insider threats are more harmful than external threats. At the same time, they mentioned that the damage they inflict can be more devastating because they are knowledgeable about issues such as the zero-day vulnerability of the hardware and software in the system, which external threats cannot have. For this reason, to ensure information security, it is necessary to increase the information security awareness of the managers and employees of the institution. To understand why raising awareness is important, mentioning the threats and risks is essential. The importance of cybersecurity and information security should be emphasized to protect personal and corporate interests. It is defined that each individual has roles and responsibilities in this regard; it should be demonstrated that individuals, institutions, and ultimately the state in general are interconnected.

Creating a cybersecurity strategy document and implementing it within the framework of an action plan is no longer just a technology-oriented security strategy. It is an international strategy that should be considered in a much more comprehensive range due to its unlimited application and scope. In Kovacs's [4] study, he mentioned that since the security of infrastructures based on information technologies, which exist in public services, economic life, public administration, defense sector, and even in the smallest detail of daily life, is of vital importance, if these systems do not work, society does not work either. At the same time, he stated that the importance of cyberspace should not be questioned in this case. For these reasons, he emphasized that the challenges and threats to cyberspace should be addressed at the strategic level. The national strategy has also become one of the critical points to be discussed in the country's defense. For these reasons, strategies and implementation methods should be developed and regularly updated to reduce risks and defend security against cybersecurity threats.

In this study, worldwide best practice examples (TR National Cybersecurity Strategy [5, 6], Singapore Cybersecurity Strategy [7-10], and Estonia Cybersecurity Strategy [11-12]) are reviewed to create a successful national cybersecurity strategy and action plan. At the same time, guidelines from organizations such as the European Network and Information Security Agency (ENISA) [13], the North Atlantic Treaty Organization (NATO) [14], and the International Telecommunication Union (ITU) [15], which is the information and communication technologies institution affiliated to the United Nations were also evaluated.

Around the world, effectiveness and implementation problems are challenges in cybersecurity strategies. Strategies may be insufficient or incomplete due to technological innovations and developing cyberspace. For this reason, the research focused on increasing the strategy's effectiveness to find solutions to these problems. For this purpose, the country strategies and the directives of organizations such as ENISA, NATO, and ITU have been examined, and a data source has been created. The generated data source and action titles were decided Using good practice examples and guidelines as crucial milestones. Unlike other studies, it has been proposed to implement the action plan systematically over a strategy model that includes control and reporting. In addition, a risk analysis-based scorecard has been designed to provide continuous improvement for the audit and reporting part of this model. In the current studies to increase the strategy's effectiveness, trainings, conferences, public service announcements, etc., mentioned promotional and efficiency-enhancing practices, or in studies based on measurement, measurements such as awareness or risk analysis for the institution are made. In this study, unlike the existing studies, it is considered to measure the performance of the cybersecurity strategy as a solution to the effectiveness and implementation problems. Measuring risk analysis together with the asset inventory containing the action titles will help evaluate the situation and eliminate the deficiencies.

The remainder of the paper is organized as follows: Section 2 describes the country strategies reviewed and how the establishment guidelines were selected to generate the data source. Section 3 examines different studies on the national cybersecurity strategy. The strategy model that will increase the effectiveness of the action plan operation is suggested in Section 4. At the same time, managerial and technical actions are also described in this section. In Section 5, the risk analysis-based scorecard can be used to develop or update strategies to tackle cybersecurity challenges internationally. In the last section, the contribution of this study is presented, and suggestions for improvements are given.

2. MATERIALS AND METHODS (MATERYAL VE METOD)

As can be seen from the Effective Strategy Development flowchart in Figure 1, this study started by examining the strategy documents and action plans of the countries (United States, Germany, China, Denmark, Estonia, France, England, Qatar, Cyprus, Korea, Romania, Russia, Singapore, and Turkey) that have strategy documents. In addition, the guidelines for strategy development and implementation by organizations such as ENISA, NATO, and ITU were also researched for their guiding nature. While the current strategy plans are essential for learning the latest methods and applications due to the developing technology, the first strategies created for the countries are crucial because they are the initial step. With the development of technology, the tools and applications used are also developing, changing, and updating at the same speed. Technological change can be observed very clearly in every field.

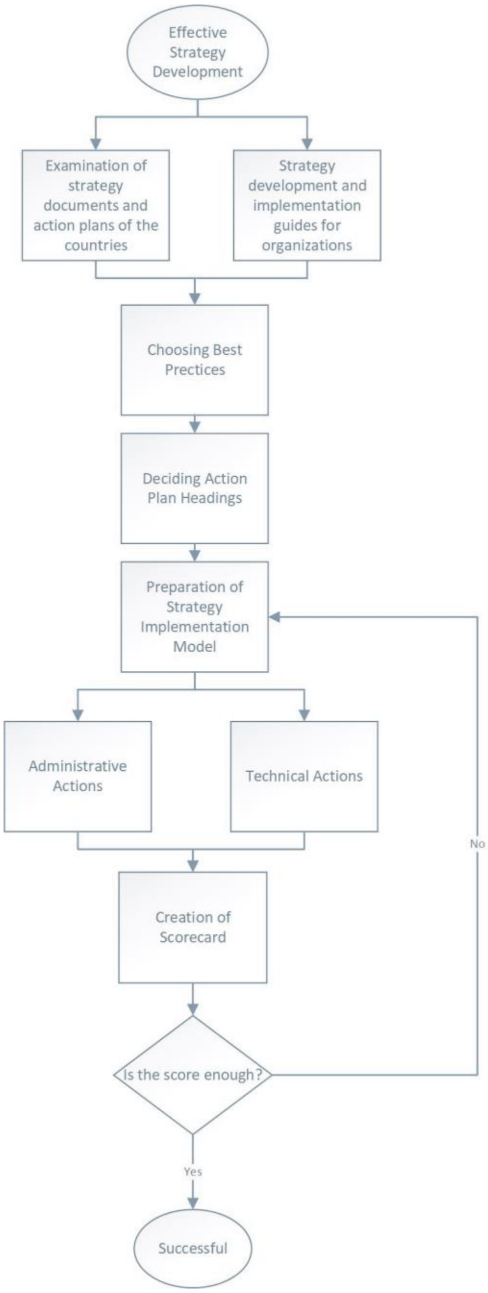
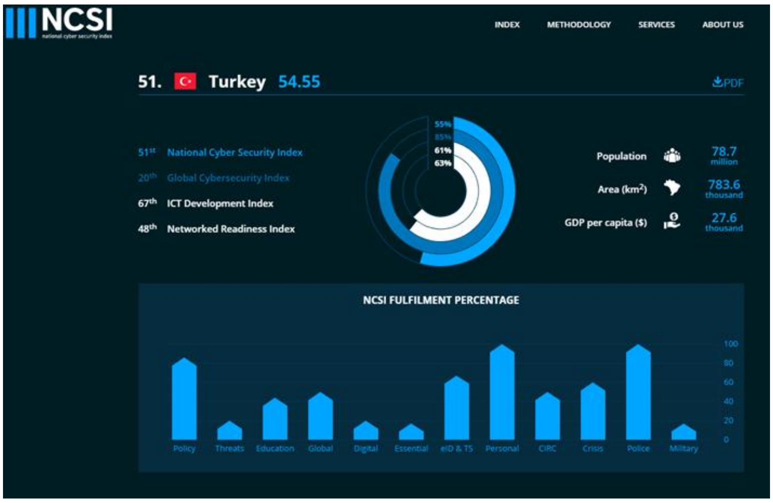

Effective Strategy Development
Examination of strategy documents and action plans of the countries
Strategy development and implementation guides for organizations
Choosing Best Prectices
Deciding Action Plan Headings
Preparation of Strategy Implementation Model
Administrative Actions
Technical Actions
Creation of Scorecard
Is the score enough?
No
Yes
Successful

Figure 1. Effective Strategy Development Flowchart (Etkili Strateji Geliştirme Akış Şeması)

Creating a strategy action plan is a crucial step to achieving its purpose. The action plan is the plan to achieve the vision of the strategy. For this reason, creating a successful strategy depends on organizing a good action plan. Examining the best examples, understanding the action plans of successful countries, developing methods to keep their applicability at the highest level, and being aware of the latest developments are the keys to a successful strategy.

This study has two reasons for choosing the National Cybersecurity Strategies of Türkiye, America, England, Estonia, and Singapore as a guide. First, they are active and constantly renewed; second, they have a good score in the Global Cyber Security Index [16-19], a reliable reference that measures global cybersecurity commitment.

Up-to-date data from all countries are available on the "National Cyber Security Index (NCSI)" website funded by the Estonian Ministry of Foreign Affairs. The NCSI is a global index that measures countries' preparedness to prevent cyber threats and manage cyber incidents. NCSI is a database of publicly available evidence materials and a national cybersecurity capacity-building tool. National cybersecurity information of 160 countries can be accessed through this map. The graphical representation of NCSI Achievement Percentage is divided into 12 sections, as shown in Figure 2. In addition, there is information such as that country's population, area, and per capita national income.



51. Turkey 54.55

51st National Cyber Security Index
20th Global Cybersecurity Index
67th ICT Development Index
48th Networked Readiness Index

Population 78.7 million
Area (km²) 783.6 thousand
GDP per capita ($) 27.6 thousand

Figure 2. National Cyber Security Index (Türkiye) (Ulusal Siber Güvenlik Endeksi (Türkiye))

All updated versions of National cybersecurity information are also available on this site. Each strategy is evaluated in 3 areas: General Cyber Security Indicators, Basic Cyber Security Indicators, Incident and Crisis Management Indicators. At the same time, it is possible to compare these global indices, which measure countries' preparedness to prevent cyber threats and manage cyber incidents, through these indicators.

Both the European Union and NATO member states considered it necessary to take steps towards cybersecurity and prepared a strategy. In addition to the strategies created by the European Union member states or NATO with cybersecurity strategies, organizations such as ENISA, NATO, and ITU also draw attention with their studies in this field.

ENISA has done a lot of work on the development and implementation of national cybersecurity strategies and has also published guidelines. It supports member states. On its web page, the strategies of the member countries are shown on an interactive map.

NATO has developed a policy and action plan approved by its allies. It regards cyber defense as the main task of the alliance. It enables further development of policy through activities such as awareness, training, and exercises among allied countries. It also undertakes information sharing, cooperation, and mutual assistance among member states.

ITU provides guidance on how countries can develop their strategies or support existing practices to make the digital environment more secure in their prepared ITU application guide.

As a result of the good practice examples and guides examined, "Action Plan Headings" for the targets of the National Cybersecurity Strategy were decided. To increase the applicability of the action plan titles, the actions are divided into two administratively and technically, and it is recommended to act according to the prepared strategy implementation model. At the same time, a scorecard was created to measure the strategy's effectiveness to be used in the strategy implementation model, audit, and reporting area.

2. NATIONAL CYBERSECURITY STRATEGY (ULUSAL SİBER GÜVENLİK STRATEJİSİ)

When creating a cybersecurity strategy and its action plan, one of the first questions that comes to mind is why a national plan should be made, not a single strategy valid for all countries. There are already standards for information security, like ISO 27001, around the world. However, the way of implementation and approach of each country may differ. As Kovacs [4] puts it, "National cybersecurity strategies, whether made by big powers or small countries, have different answers to the challenges of cyberspace." For this reason, each country should develop its strategy according to its structure, capabilities, and awareness level.

There are different explanations for why a national cybersecurity strategy is needed. One of the best descriptors has been made by Haddad and Binder [20]. According to them, new cybersecurity regimes are required to protect them from the risks and threats that may occur as society is increasingly intertwined with digital technology. At the same time, they talk about the vision of the future and the problems arising from new threats and insecurities as a significant challenge in digitalization and become the government's responsibility. As they mentioned, digitalization is intertwined with society. "National Cybersecurity Strategies" are needed to adapt and trust digital technology, to be protected from risks and threats, and to create a defense mechanism against external threats.

In the literature review, the most striking studies are the comparative studies using the guideline documents prepared by ENISA, NATO, and ITU. For example, in his research, Karatas [21] compared the cybersecurity strategies of Turkey, the United States of America, and the United Kingdom by using the headings in the cybersecurity strategy preparation guides put forward by the European Union Network and Information Security Agency (ENISA) and the International Telecommunication Union (ITU). He mentioned that although the USA is one of the strongest countries regarding systems and infrastructure against cyber threats, the implemented programs, systems, and infrastructures still need to be improved against today's dangers.

In his study, Stitilis [22] compared the cybersecurity policies of the EU and NATO countries. They pointed out that the EU and NATO cybersecurity strategic documents differ in scope and emphasis. They mentioned that all strategies are different and that it is too early to create a unified national cybersecurity strategy model (a single document) applicable to all countries.

Göçoğlu and Aydın [23] examined the official cybersecurity policies of the USA, Russia, and China and made a comparative analysis. They also mentioned in this study the importance of determining roles within the framework of Haddad and Binder's [20] security policies. In addition, according to the International Telecommunication Union, the cybersecurity ratings of these three countries are given. It is mentioned that by producing its information technology, China is avoiding the hegemony of the leading countries in the sector and aims to maintain its national sovereignty. They noted that the steps the USA, Russia, and China took for a solid and successful cybersecurity policy spanned 20 years. They also said that Turkey can be successful in this area by taking important steps with rapid structural reforms and appropriate policies.

In the study by Egas et al. [24], Ecuador, a developing country, was chosen as a case study, and ENISA and ITU were taken as the basis for this review. Considering the characteristics of developing countries, they conducted a study investigating whether it would be possible to detail a proposal for a national cybersecurity document that serves as a guide and includes current good practices. In the study, it has been mentioned that the fight against cyber threats is dealt with within the framework of existing tools and capacities in combating these threats. However, the situation is similar for developed or developing countries due to their transnational nature. He also stressed that developing the capacity and skills to locally, efficiently, and effectively manage the growing number of cybersecurity-related incidents affecting the country's progress is vital. In this respect, university interventions should be a pillar to ensure technological autonomy through education, research, and innovation.

In his doctoral thesis, Al-Hamar [25] conducted research to improve the information security processes of Qatari organizations by developing a comprehensive Information Security Management framework applicable to the implementation of the National Information Assurance (NIA) policy, taking into account the culture and environment of Qatar. Many literature reviews, surveys, interviews, and similar studies have been carried out to achieve the research purpose. In this research, the lack of security culture, lack of awareness, lack of trained personnel in information security, and the existing obstacles in the current system that need to be addressed are mentioned.

The doctoral study by Alarifi [26] examined the assessment and mitigation of information security risk in Saudi Arabia. This thesis has studied the information security awareness level among the public and the information security practices among the IT departments of organizations in Saudi Arabia. According to the results of online surveys, a new information security model has been developed, and it has been stated that this new model will protect and improve the awareness and practice of information security in Saudi Arabia in the short and long term.

In his doctoral thesis, "An Experimental Study on Information Security Policies, Information Technology Management and International Standardization Security Certification Organization" by Paarlberg [27] investigated the benefits of developing and maintaining an information security policy for an organization and whether this benefit is measurable. Izycki and Colli [28] mention that among the 86 strategies they reviewed, 58 countries listed the protection of critical infrastructures as one of the cybersecurity goals at the national level, and a comparative analysis between strategies mentions that the safety of their critical infrastructure is the third most frequent strategic goal. Pavlon [29] mentioned in his study that evaluating and understanding the organization's security culture can lead to an understanding of how security effectiveness can be maintained and to identify security vulnerabilities that can lead to downtime or cause failure. Therefore, he mentioned that approaches to developing a security culture will lead to an increase in trust and a decrease in cyberattacks and their effects. Darıcılı [30] examined Turkey's "National Cybersecurity Strategy and Action Plan" in his study titled "Analysis of Turkey's Cybersecurity Policies". It compared the 2013-2014 National Cybersecurity Strategy and Action Plan [5] with the 2016-2019 National Cybersecurity Strategy and Action Plan [6]. He mentioned that the two strategies are compatible, but the second strategic planning is simpler and more general. He especially said that more emphasis is placed on developing national software and technologies. At the end of the study, it was especially emphasized that there is an awareness in the state administration of Turkey about developing the country's cybersecurity strategy and investing in cyber defense and attack capacity, but these steps should be designed further.

One of the reasons the strategies are inefficient is the lack of institutional structure and the lack of or incomplete distribution of responsibilities. Haddad and Binder [20] mention that duties are not distributed, and there needs to be an institutional structure in the Information and Communication Security Strategy, which was first prepared in their study in Austria. To overcome these problems, they stated that a framework with different duties and responsibilities has been established in the next Austrian Cybersecurity Strategy. In the same study, they mention two critical programs in the Austrian security research sector to maintain digital security and security through R&D. These are the ministry-funded security research program KIRAS and the Austrian Security Research (Horizon 2020). Several programs have been launched in Austria to increase digital awareness and practical knowledge. These include assistance for Small and Medium Enterprises, financing schemes to improve digital structures, and training courses to transform unskilled citizens and the workforce into digitally viable and prudent issues [20]. In the Austrian policy vision, creating digitally conscious and sensitive issues is not only a matter of vocational training and continuing skills development. Still, it should also be diffused into the education system. With these efforts, besides having the ability to reduce risks and respond appropriately to threats, it also helped to train qualified personnel. As a result of all these, according to Haddad and Binder, the number of cybersecurity experts in Austria is expected to increase. It aims to increase resilience by creating practical expertise through simulated events and exercises to upgrade digital safety and security.

Countries have different approaches when designing and developing the National Cybersecurity Strategy. While some of them mentioned these approaches in the action plan, some did not make any explanation about it. Santisteban et al. [31] have analyzed the National Cybersecurity Strategies and divided the development of a strategy into 5 phases: Initiation, Inventory and Analysis, Production, Execution, Monitoring, and Evaluation.

3. NATIONAL CYBERSECURITY STRATEGY ACTION PLAN (ULUSAL SİBER GÜVENLİK STRATEJİSİ EYLEM PLANI)

The action titles that must be among the guidelines and the country strategies examined were decided according to the number of countries using these titles and the explanations in the guides or strategies. While developing the national cybersecurity strategy, it is essential to include the topics listed in Table 1 within the action headings, even if they are outside the target headings for the strategy to succeed.

Table 1. National Cybersecurity Strategy Goals (Ulusal Siber Güvenlik Stratejisi Hedefleri)

Action Headlines	Countries	Number of Countries
Risk Analysis of Critical Infrastructure	USA, Germany, Estonia, Southern Cyprus, Singapore, Romania, Turkey	8
Protecting Critical Infrastructure	USA, Germany, China, Denmark, Estonia, Southern Cyprus, England, Qatar, Romania, Singapore, Turkey	11
Legislation	China, Germany, Estonia, England, Qatar, Romania, Singapore, Turkey, Southern Cyprus	10
Fighting Cybercrime	USA, Germany, China, Denmark, Estonia, France, Cyprus, England, Qatar, Korea, Romania, Singapore, Turkey	13
Public-Private sector cooperation	USA, Germany, Estonia, Denmark, Southern Cyprus, England, Qatar, Korea, Romania, Singapore, Turkey	12
International Cooperation	USA, Germany, China, Denmark, Estonia, France, UK, Korea, Romania, Singapore	10
Awareness	USA, Germany, China, Denmark, Estonia, France, Cyprus, Qatar, Romania, Singapore, Turkey	11
Research & Development	Denmark, Estonia, Southern Cyprus, England, Qatar, Romania, Singapore, Turkey	9
Drill	Denmark, Cyprus, Qatar, Singapore, Türkiye	5

Having a good security strategy or implementing a good strategy first passes through learning, assimilation, and culturally appropriate examples of good practice around the world. While choosing good practice examples, looking at the updated years of the strategies and the strategy titles that should be in the strategy is necessary. In this study, three countries were selected as good practice practices. First, Turkey was chosen because it updates its strategies regularly and has a strategy that covers the current time. Secondly, Estonia has been chosen because it is effectively implemented, has been intertwined with cybersecurity for a long time, constantly updates itself, and is a pioneer in this field. The third country, Singapore, was chosen because of its master plans that support the strategy plan it prepares for each new year (2018, 2020, 2021) and the technology it follows to increase awareness and applicability. Because cybersecurity is a formation intertwined with technology, current strategy plans are essential.

For the National Cybersecurity Strategy to be put into practice, it is necessary to follow the developments in the field of cybersecurity, take into account the technological situation of the country, and act with a well-prepared action plan without ignoring threats and risks. In the action plan, the case should be evaluated, assets and risks should be determined, necessary mechanisms should be established to protect assets and manage risks, and the action plan should be followed and coordinated.

The mission and vision of the National Cybersecurity Strategy should be understood and implemented starting from the highest levels of the state. Thus, the importance given to strategy as a country will be better understood, and its applicability will increase simultaneously. One of the critical aspects of the development and successful implementation of the National Cybersecurity Strategy Paper is collaboration between stakeholders. Al-Ghamdi [32] mentions in his study that identifying and involving all relevant stakeholders in developing and successfully implementing the National Cybersecurity Strategy is essential. However, daunting tasks and understanding stakeholder needs and their unique knowledge and expertise will facilitate collaboration toward achieving the strategy's objectives. It also emphasizes that monetary and social incentives will increase the implementation of the strategy. American Public Policy Research Institute researcher Tews [33] held a "web event on whether the United States needs a national cybersecurity strategy." His web blog included critical evaluations of Jim Dempsey, Jim Lewis, Sujit Raman, and Diane Rinaldo that stood out from this event. Diane Rinaldo, one of the debaters, said that the legislation alone is not sufficient and that there is no single way to progress in the field of national cybersecurity; she wrote that at the end of the day, it's essential to have all voices in the hall to help ensure the best legislation moves forward. In the same discussion panel, Jim Lewis said that deterrence is critical for national cybersecurity, but it often doesn't work. The reason for non-operation is that there is no legally binding and international cooperation to be feared. For this, he mentioned that the norms will regularize cyber operations by placing them under the umbrella of international law or humanitarian law and that deterrence can be ensured through accountability. Jacuch [34], in his study comparing Polish and selected country strategies, mentions that most countries emphasize the need for the government to cooperate with the private sector and the academic community. When the studies on creating, taking action, updating, or comparing different strategies are examined, it is understood that it should be in an easily applicable and measurable planning. In this study, a model was created to meet this need, as shown in Figure 3.

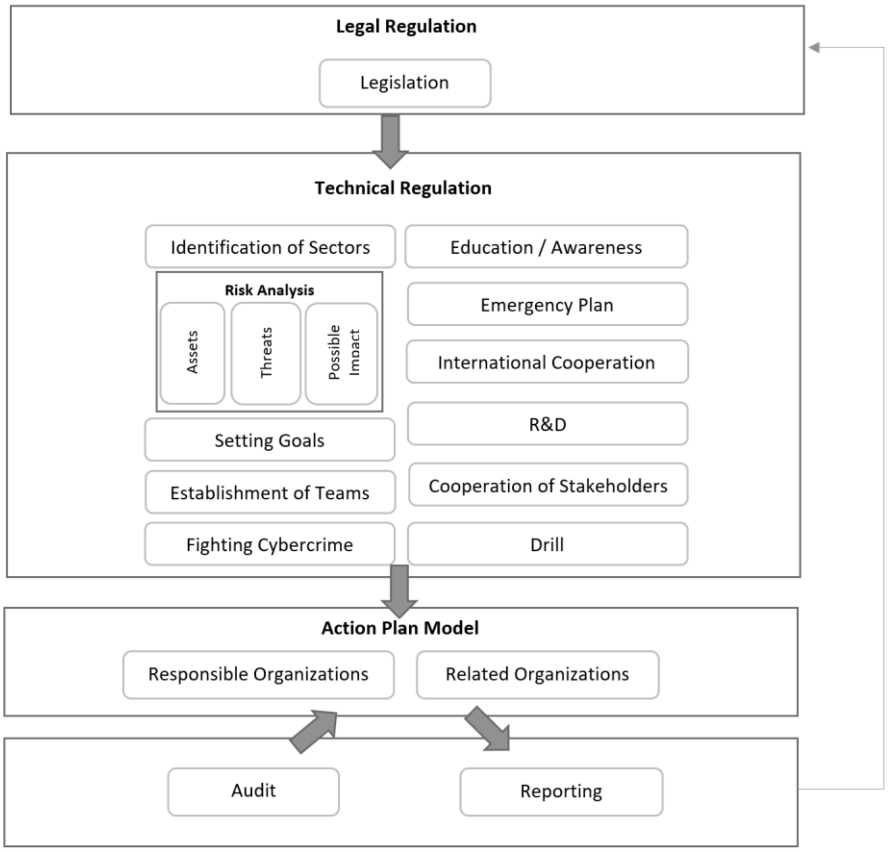


Figure 3. Strategy Implementation Model Recommendation (Strateji Uygulama Modeli Önerisi)

While creating this model, the PDCA model [35], one of the well-known dynamic models used for the continuous improvement of processes, was taken as an example. The PDCA (Plan-Do-Check-Act) model is a systematic way of managing quality and continuously provides steps to improve processes, as seen in Figure 4. Media can be the simplest example of why continuous improvement is necessary. As the popularity of new media increases, many companies are shifting their advertising budgets from traditional media to areas such as social media [36]. For example, while public service announcements broadcast on television were a vital communication method in the past, it has become more critical to broadcast public service announcements over social media, organize digital competitions, and prepare digital campaigns to communicate using technology.

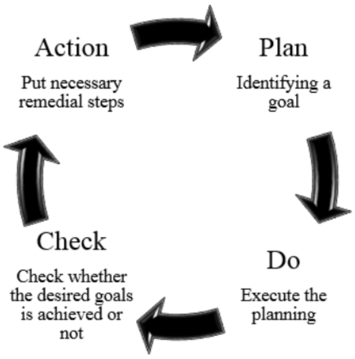

Action
Put necessary remedial steps
Plan
Identifying a goal
Do
Execute the planning
Check
Check whether the desired goals is achieved or not

Figure 4. Strategy Implementation Model Recommendation (Strateji Uygulama Modeli Önerisi)

Adhering to the model proposed in this study can increase both ease of application and efficiency. In addition, with the audit and reporting section in the strategy action plan, targets and action titles can be measured, and a self-monitoring and improving structure can be provided.

In the cybersecurity strategy action plan, there are technical actions as well as administrative formations. In this study, we consider the action plan in 2 parts, Administrative and Technical Actions, to ensure national cybersecurity, increase its applicability, raise awareness, and ensure the strategy can work.

3.1. Administrative Actions (İdari Eylemler)

To ensure the functionality of the technical actions, the administrative structure must first be established and made operational among the steps to be taken in the action plan. Implementing the action plan requires identifying stakeholders, establishing legal regulations, establishing incident response teams, and especially establishing a Cybersecurity Board that will coordinate the entire structure. Administrative actions can be listed as follows:

- Legislation: One of the cornerstones of the creation and execution of the strategy, and even the most important, is to be supported by a legal framework.
- Identifying Stakeholders: To have an effective and successful strategy and increase the action plan's applicability, it is crucial to identify and include the stakeholders at every stage.

Establishment of Incident Response Teams: In cybersecurity breaches, early detection of incidents, rapid intervention, and reactivation of working systems will keep the damage to a minimum.

3.2. Technical Actions (Teknik Eylemler)

With the implementation of administrative actions, the necessary organizational structure is created for the action plan to function. After the institution responsible for the strategy decides how the structure will be hierarchically from top to bottom and how it will act, the actions that need to be taken from a technical point of view start to be taken.

- Identification of Sectors and Services: It is necessary to determine the sectors and services that use the cyber world, provide services in this field, or use the service. To be protected from threats in the cyber world, it is necessary to answer the questions of what are online services, who are the organizations or private sectors that provide these services, and in which area the service is provided. In addition, the responsible institution for each sector should be determined.
- Risk analysis: After identification, the assets need to be listed. The size of the risk should be scaled, taking into account the threats to the assets and the existing vulnerabilities. The more assets there are, the more threats can be encountered, so the more vulnerable you are, the greater the risk. One of the critical points is dealing with the unknown. Therefore, it is crucial to protect assets based on what is known. The protection of critical infrastructure should be given priority when performing risk analysis. The study by Izyck and Colli [28], which analyzes and compares national cybersecurity strategies in terms of similarities shown in the scope of protection of critical infrastructures, divides the definition of critical infrastructures into two parts. The first is "Services and facilities (infrastructure) used by the community," and the second is "Infrastructures, the disruption or failure of which can be considered critical with adverse consequences to the public." is in the form.
- Setting Goals: The cybersecurity strategy should have objectives supported by the

action plan, considering technological developments and cybersecurity threats.

- Emergency Plan: Emergency plans should be prepared against cyber threats, even necessary mechanisms should be established, and checks should be made whether the system is working.
- Fighting Cybercrime: Technological events are changing almost every minute; developing and new technologies are included in our lives. However, cybercrime, a new type of crime, also changes with technology, develops and new ones emerge. Since cybercrimes have a different structure from known crimes and do not require physical contact, the current legal system is insufficient to punish these crimes.
- Awareness Training: The most essential factor in personal or corporate information breach incidents is employees' lack of awareness about security. As mentioned before, starting from the fact that the weakest link is human, the first step of the studies to be carried out in the field of cybersecurity should be training and awareness studies.
- Information Sharing and Reporting: To take cybersecurity protection to the next level, information sharing should be ensured in both national and international collaborations. All incidents must be accurately collected, reported, and shared among stakeholders. The more information is shared and informed on technological developments, threats, incidents, or losses, the more protection will increase.
- Research & Development: To have a good place in cybersecurity depends on following and developing innovations in this field and even creating and using their national technologies. Also, the private sector should be encouraged to work in this field, and even resources should be provided if possible.
- International Cooperation: Since the cyber world is a borderless medium, understanding the threats, finding the criminal, or reaching the source of the crime, especially in the fight against cybercrime, will be more successful with international cooperation. In addition, technological developments differ from country to country. Being aware of the changes and approaches in different countries will add value to each country's cybersecurity field.
- Drill: It is one of the inevitable actions to organize drills in specific periods to be able to fight cybercrime, be ready in emergencies, and react quickly. The drill is an application that measures readiness for actual attacks. Chatchalermpun and Daengsi [38], in their article "Raising cybersecurity awareness using phishing attack simulation," demonstrated that cyber drills and cybersecurity knowledge sharing can increase cybersecurity awareness in a financial institution, a targeted industry for attackers. They mentioned that thanks to the understanding gained, risks or threats can be reduced, and the possibility of timely intervention can be increased.

4. SCORECARD BASED ON RISK ANALYSIS (RİSK ANALİZİNE DAYALI PUAN KARTI)

ENISA has created the National Cybersecurity Strategies Assessment Tool (ENISA) [39] to help member states evaluate their strategic priorities and objectives regarding their National Cybersecurity Strategies. With this tool, the cybersecurity priorities of the countries are selected. Then, by answering a few simple questions (with YES or NO), ideas and advice can be sought, and improvements can be made. In this tool created by ENISA, there are 15 targets and different numbers of questions that test each target. Some of the targets are listed as “Develop contingency plans," "Protect critical infrastructure," "Organize drills," "Create reporting mechanisms," "Increase user awareness," "Encourage R&D” and “Strengthening training."

Shabe et al. [40] discussed a scorecard approach to present the results of measures of cybersecurity awareness levels among mobile phone users. They noted that scorecards should be used to research cybersecurity issues in other areas in South Africa. They also emphasized that the scorecard could serve as a guide for planning future campaigns to address gaps in awareness of cybersecurity issues. In his blog post, Null [41] mentioned that Dun & Bradstreet Corporation, an American company that provides business data, analytics, and insights, has even added a Cyber Risk Rating product to their business information offerings. He also mentioned that "Existing and Planned Control" and "Value of Assets" must be within the scope of the evaluation while creating the risk score. Venkataraman [42], in his article titled "The Importance of Measuring

Security Awareness" for Forbes magazine, mentioned that by spending time and effort to measure the success of security awareness practices and sharing this information, a better understanding and appreciation of the security role of the organization could be achieved. He also emphasized in the last word that "Great programs will only succeed thanks to analytics, insights, and actionable data." Jazri et al. [43] proposed a measure index of this cybersecurity goodness by analyzing the vital signs of critical organizations, taking into account the 114 vital signs recommended by the ISO/IEC 27001 standard.

Considering that technology changes every moment during the creation or implementation of the strategy, it needs to be continuously improved. Research has been conducted on different ways and methods to design, develop, and effectively implement the National Cybersecurity Strategy. In some studies, it was emphasized that the effectiveness of awareness training would be increased, while in some studies, it was mentioned that the deterrence or defense aspect should be strengthened. However, the difficulty of implementing the cybersecurity strategy, a global problem increasing exponentially with each passing day, still needs to be solved. To close this gap in the literature, the Audit and Reporting sections of the Strategy Implementation Model proposed in this article are considered.

As in creating the Strategy Implementation Model proposal, the PDCA model was taken as an example to support the continuous improvement of the processes, and a scorecard was designed to be used in the audit section. While creating this scorecard, ENISA's assessment tool was taken as a basis. In the international ISO 27001 standard, which specifies the requirements for establishing, implementing, maintaining, and continuously improving an information security management system, the items specified explicitly in the information security risk assessment section were also used. Some of the things used in the scorecard are to define information security risks, identify risk owners, etc., listed in this standard's information security risk assessment process. Also, to provide improvement, it was started from being able to show mathematically whether a security policy works or not. To evaluate at this stage, it is necessary to find an answer to the question of what should be measured. At this point, fundamental performance indicators were selected by considering the risk levels determined due to the risk analysis and the implementation of the action titles in the action plan.

Table 2. Scorecard (Puan kartı)

Actions	Risk Degree	Fulfilling Action Titles	Responsible Institution		Periodic Evaluation	Total
Cybersecurity Board	Middle (12-15)	Yes	☒ Yes	☐ No	Yes	86,7
Legislation	Low (6-10)					90,0
Cyber Crime	Very low (1-5)	No	☒ Yes	☐ No	Yes	
Laws, regulations	Middle (12-15)	Yes	☒ Yes	☐ No	Yes	
Cooperation of Stakeholders	Very low (1-5)					100,0
Identifying Stakeholders	Very low (1-5)	Yes	☒ Yes	☐ No	Yes	
Public-Private sector cooperation	Very low (1-5)	Yes	☒ Yes	☐ No	Yes	
Identification of Sector Services	High (16-20)					85,0
Critical Infrastructures Identification	High (16-20)	Yes	☒ Yes	☐ No	Yes	
Critical Infrastructure Responsible	Middle (12-15)	Yes	☒ Yes	☐ No	Yes	

The indicators in the scorecard shown in Table 2 were created using the strategy implementation model. Each indicator is scored separately and according to different weights. Key Performance Indicators (KPIs) and their weights are as follows:

- Risk Degree: 20%
- Fulfilling Action Titles: 40%
- Responsible Institution: 20%
- Periodic Evaluation: 20%

In Key Performance Indicators, risk grade is calculated by probability and severity of impact. The action titles are fulfilled by a single Yes or No question for each action. The Yes or No questions evaluate whether the action titles have a Responsible Institution. For the periodic evaluation, a period must be determined before scoring, and whether the monitoring is done according to that period is also measured with Yes or No questions. Fulfilling the action titles is directly linked to the strategy. Action titles can be fulfilled without a responsible institution, periodic evaluation, or risk analysis. Therefore, fulfillment of action titles has a higher percentage than other indicators. Risk Level, Responsible Institution, and Periodic Evaluation indicators have equal percentages.

5. CONCLUSIONS (SONUÇLAR)

Although the examined countries have national cybersecurity strategies, they are still exposed to cyber-attacks. When the existing strategies are discussed, it is revealed that the action plan prepared for the strategy's success needs to be fully complied with or implemented effectively. Some countries offer efficiency-enhancing plans yearly without waiting for the strategy life cycle.

To prepare an effective national cybersecurity strategy, first of all, field research should be done well. Assets and services related to technology must be identified, and risk analysis must be made. The action plan should be divided into two managerial and technical actions, considering the strategy implementation model, and should be implemented gradually. In addition, auditing and reporting should be done as suggested in the strategy implementation model, and a scorecard should be used to measure the strategy's success and ensure its sustainability.

In this article, it is mentioned for the first time that the strategy model was prepared to eliminate the lack of strategy implementation and the evaluation of the prepared action plan using the scorecard. Thanks to the proposed strategy implementation model, the stages of cybersecurity strategy formation will develop in a correct plan and hierarchically from top to bottom. The proposed strategy implementation model will assist in developing the cybersecurity strategy in an accurate plan and hierarchically from top to bottom. The scorecard, which will shed light on the extent to which the action plan titles have been fulfilled and will also provide information on auditing and reporting, which is the last stage of the strategy implementation model, may also help other countries. The non-working aspects of the strategies and the actions that need to be added or developed will quickly emerge. In addition, the information obtained with the guides and good practice examples examined in this study will also help countries that want to build a strategy. Using the risk analysis recommended for information resources in the standard of establishment, implementation, maintenance, and continuous improvement of the information security management system (ISO 27001) as a part of this study will increase its effectiveness and ensure its sustainability.

In current studies, promotion and productivity-enhancing practices such as training, conferences, and public service announcements are mentioned to increase the strategy's effectiveness. In one of the existing metrics-based studies, cybersecurity awareness among phone users was measured using a scorecard. Only the specified titles were given points in the study. Another study mentioned the importance of conducting risk analysis only for the institution. In a study aimed at measuring awareness, the importance of noticing the attack, avoiding the attack, or measuring the number of reactions to the threat was mentioned. In another study to measure the goodness of cybersecurity, measurement was made using the fundamental variables of ISO 27001. In this study, unlike the existing studies, measuring the performance of the cybersecurity strategy is seen as a solution to the productivity and implementation problems. Making an inventory of assets will help determine the security areas that need to be protected and increase security. In addition, creating scores using risk analysis will increase the reliability of the measurements. Identifying assets, seeing risk, and identifying gaps will help approach a more secure system. A limited number of countries is seen as a limitation in this study. The study can be improved by selecting more countries. The strategy's action plan can be updated in the future by using the information obtained from the breaches and data losses. By creating a technological system and collecting data, the strategy can be improved, and its effectiveness can be increased simultaneously.

As a result, while developing a national cybersecurity strategy or updating the existing strategy, attention should be paid to ensure that the strategy is effective, constantly evolving, and reinforcing weak points. A successful strategy must be fed with feedback, measured, and continuously improved.

DECLARATION OF ETHICAL STANDARDS (ETİK STANDARTLARIN BEYANI)

The author of this article declares that the materials and methods they use in their work do not require ethical committee approval and/or legal-specific permission.

Bu makalenin yazarı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

AUTHORS' CONTRIBUTIONS (YAZARLARIN KATKILARI)

Özlem EVRE**:** She did the conceptualization, formal analysis, and writing. Kavramsallaştırmayı, biçimsel analizi ve yazma işlemini yaptı.

Bünyamin CİYLAN**:** He did the conceptualization, review and supervision. Kavramsallaştırmayı, incelemeyi ve denetlemeyi yaptı.

CONFLICT OF INTEREST (ÇIKAR ÇATIŞMASI)

There is no conflict of interest in this study.

Bu çalışmada herhangi bir çıkar çatışması yoktur.

REFERENCES (KAYNAKLAR)

[1] Tsaruk O, Korniiets M. Hybrid nature of modern threats for cybersecurity and information security. Smart Cities and Regional Development (SCRD) Journal. 2020; 4(1): 57-78.

[2] Flowerday S, Tuyikeze T. Information security policy development and implementation: The what, how and who. Computers & Security. 2016; 61: 169-183.

[3] Mills J, Stuban SMF, Dever, J. Predict insider threats using human behaviors. IEEE Engineering Management Review. 2017; 45(1): 39-48.

[4] Kovacs L. National cybersecurity strategy framework. Academic and Applied Research in Military and Public Management Science. 2019: 18(2).

[5] TR Ministry of Transport, Maritime Affairs and Communications. National cyber security strategy and 2013-2014 action plan. 2013. Available online: https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf (accessed on 12 June 2023).

[6] TR Ministry of Transport, Maritime Affairs and Communications. 2016-2019 national cyber security strategy. 2016. Available online: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/2016-2019guvenlik.pdf https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf (accessed on 12 June 2023).

[7] Cyber Security Agency of Singapore. Singapore's cybersecurity strategy. 2016. Available online: https://www.csa.gov.sg/Tips-Resource/publications/2016/Singapore-Cybersecurity-Strategy (accessed on 12 June 2023).

[8] Cyber Security Agency of Singapore. Singapore's safer cyberspace masterplan. 2020. Available online: https://www.csa.gov.sg/Tips-Resource/publications/2020/safer-cyberspace-masterplan (accessed on 12 June 2023).

[9] Cyber Security Agency of Singapore. Singapore cyber safety handbook. 2020. Available online: https://www.csa.gov.sg/docs/default-source/csa/documents/publications/cyber-safety-activity-book-and-handbook/cyber-safety-handbook.pdf?sfvrsn=7ddf002f_0 (accessed on 12 June 2023).

[10] Cyber Security Agency of Singapore. The singapore cybersecurity strategy. 2021. Available online: https://www.csa.gov.sg/docs/default-source/csa/documents/publications/the-singapore-cybersecurity-strategy-2021.pdf?sfvrsn=809ced95_0 (accessed on 12 June 2023).

[11] Republic of Estonia. Cybersecurity strategy. 2019. Available online: https://www.mkm.ee/media/703/download (accessed on 12 June 2023).

[12] Republic of Estonia. Cybersecurity strategy in Estonia. 2021. Available online: https://www.ria.ee/media/1494/download (accessed on 12 June 2023).

[13] The European Network and Information Security Agency (ENISA). National cyber security strategies practical guide on development and execution. 2012. Available online: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide (accessed on 12 June 2023).

[14] NATO Cooperative Cyber Defense Centre of Excellence. National cyber security framework manual. 2012. Available online: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf (accessed on 12 June 2023).

[15] International Telecommunication Union (ITU). Guide to developing a national cybersecurity strategy. 2018. Available online: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf (accessed on 12 June 2023).

[16] International Telecommunication Union (ITU). Global cybersecurity index. 2014. Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed on 12 June 2023).

[17] International Telecommunication Union (ITU). Global cybersecurity index. 2017. Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed on 12 June 2023).

[18] International Telecommunication Union (ITU). Global cybersecurity index. 2018. Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed on 12 June 2023).

[19] International Telecommunication Union (ITU). Global cybersecurity index. 2020. Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed on 12 June 2023).

[20] Haddad C, Binder C. Governing through cybersecurity: National policy strategies, globalized (in-) security and sociotechnical visions of the digital society. Österreichische Zeitschrift für Soziologie, 2019; 44(1):115-134.

[21] Karatas A. The comparative analysis of national cyber security policies: United States, United Kingdom and Turkey examples. Journal of Academic Social Resources, 2020; 5(19): 737-751.

[22] Stitilis D, Pakutinskas P, Malinauskaitė I. EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. Security Journal. 2017; 30(4): 1151–1168.

[23] Göçoğlu V, Aydın MD. Cybersecurity Policy: A comparative analysis of the USA, Russia, and China. Journal of Security Sciences. 2019; 8(2): 229-252.

[24] Egas MR, Ninahualpa G, Molina D, Ron M, Ninahualpa G, Díaz J. National cybersecurity strategy for developing countries: Case study: Ecuador proposal. In proceedings of the 15th Iberian Conference on Information Systems and Technologies (CISTI), Sevilla, Spain. 24-27 June 2020.

[25] Al-Hamar A. Enhancing information security process in organisations in Qatar. PhD Thesis, Loughborough University, England, 25 June 2018.

[26] Alarifi AS. Assesing and mitigating information security risk in Saudi Arabia. PhD Thesis, University of Wollongong, Australia, 2013.

[27] Paarlberg JW. An empirical analysis on the effectiveness of information security policies, information technology governance, and international organization for standardization security certification. PhD Thesis, Capella University, United States, 2016.

[28] Izycki E, Colli R. Protection of critical infrastructure in national cyber security strategies, european conference on cyber warfare and security. In proceedings of the 18th European Conference on Cyber Warfare and Security – ECCWS, Coimbra, Portugal, 4-5 July 2019.

[29] Pavlova E. Enhancing the organisational culture related to cyber security during the university digital transformation. Information & Security. 2020; 46(3): 239-249.

[30] Darıcılı AB. Analysis of Turkey's cyber security policies; Turkey's potential cyber security strategy. Turkish Journal of TESAM Academy. 2019; 6(2): 11-33.

[31] Santisteban A, Cunyarachi LO, Andrade-Arenas L. Analysis of national cybersecurity strategies. (IJACSA) International Journal of Advanced Computer Science and Applications. 2020; 11(12): 771-779.

[32] Al-Ghamdi M. Guide to developing a national cyber security strategy. Materials Today: Proceedings. 2021.

[33] Tews S. Does the US need a national cybersecurity strategy? 2021. Available online: https://www.aei.org/events/does-the-us-need-a-national-cybersecurity-strategy/ (accessed on 12 June 2023).

[34] Jacuch A. Comparative analysis of cybersecurity strategies. European Union Strategy and Policies. Polish and Selected Countries Strategies. Online Journal Modelling the New Europe. 2021; 37: 102-120.

[35] Jelenc L, Lerner S, Knapic V. Strategy deployment using PDCA cycle. In Proceedings of the 5th International Scientific Conference Lean Spring Summit, Zagreb, 25 June 2020.

[36] Traditional media vs. new media: Which is beneficial. Available online: https://www.techfunnel.com/martech/traditional-media-vs-new-media-

beneficial/#:~:text=New%20media%20tends%20to%20be,interaction%20between%20business%20and%20consumer (accessed on 12 June 2023).

[37] Alauddin N, Yamada S. Overview of deming criteria for total quality management conceptual framework design in education services. Journal of Engineering and Science Research. 2019; 3(5): 12-20.

[38] Chatchalermpun S, Daengsi T. Improving cybersecurity awareness using phishing attack simulation. In proceedings on Annual Conference on Computer Science and Engineering Technology (AC2SET), Medan, Indonesia, 23 September 2020.

[39] ENISA national cybersecurity strategies evaluation tool. Available online: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool (accessed on 12 June 2023).

[40] Shabe T, Kritzinger E, Loock M. Scorecard approach for cyber-security awareness. In proceedings of International Symposium on Emerging Technologies for Education, Cape Town, South Africa, 20-22 September 2017.

[41] Null, C. What is a cyber risk score? 2021. Available online: https://www.tanium.com/blog/what-is-a-cyber-risk-score-and-why-does-it-matter/ (accessed on 28 July 2023).

[42] Venkataraman S. The importance of measuring security awareness. 2021. Available online: https://www.forbes.com/sites/forbestechcouncil/2021/10/22/the-importance-of-measuring-security-awareness/?sh=2989d26c2704 (accessed on 28 July 2023).

[43] Jazri H, Zakaria O, Chikohora E. Measuring cybersecurity wellness index of critical organisations. In proceedings of IST-Africa Conference, Gaborone, Botswana, 09 - 11 May 2018.