electronics

MDPI

Article

Information Systems Strategy and Security Policy: A Conceptual Framework

Maria Kamariotou and Fotis Kitsios *

Department of Applied Informatics, University of Macedonia, GR54636 Thessaloniki, Greece
* Correspondence: kitsios@uom.gr

Abstract: As technology evolves, businesses face new threats and opportunities in the areas of information and information assets. These areas include information creation, refining, storage, and dissemination. Governments and other organizations around the world have begun prioritizing the protection of cyberspace as a pressing international issue, prompting a renewed emphasis on information security strategy development and implementation. While every nation's information security strategy is crucial, there has not been much work conducted to define a method for gauging national cybersecurity attitudes that takes into account factors and indicators that are specific to that nation. In order to develop a framework that incorporates issues based on the current research in this area, this paper will examine the fundamentals of the information security strategy and the factors that affect its integration. This paper contributes by providing a model based on the ITU cybersecurity decisions, with the goal of developing a roadmap for the successful development and implementation of the National Cybersecurity Strategy in Greece, as well as identifying the factors at the national level that may be aligned with a country's cybersecurity level.

Keywords: strategy; information systems; security; policy; cybersecurity

Citation: Kamariotou, M.; Kitsios, F. Information Systems Strategy and Security Policy: A Conceptual Framework. *Electronics* **2023**, *12*, 382. https://doi.org/10.3390/electronics12020382

Academic Editors: Juan M. Corchado, Byung-Gyu Kim, Carlos A. Iglesias, In Lee, Fuji Ren and Rashid Mehmood

Received: 11 December 2022
Revised: 3 January 2023
Accepted: 10 January 2023
Published: 11 January 2023

1. Introduction

Information and communication technologies (ICTs) have formidable strength to advance the lives of several individuals [1–3] and promote economic development [4,5]. ICTs generate opportunities for several individuals, firms, and nations around the world [6–9]. However, with the advent of assorted technology for useful software programs and, in general, "humanitarian" technology, there is a high demand for instruments to recognize the kinds of methods that are very efficient in determining effect and sustained viability.

Some security details, such as susceptibility evaluation of current and recently added devices and actual warning and reduction of security threats, are not tackled, making those solutions incapable of dealing with advanced cybersecurity threats. This can lead to a great loss of income and repute of an organization; for example, small and medium-sized enterprises (SMEs), whose diverse and perhaps extensive substructure is practically unfeasible to maintain and manage, making them susceptible to cyberattacks. While cybersecurity methods and actions increase, social engineering assaults are becoming more predominant by taking advantage of human susceptibilities, which are difficult to identify and alleviate in a mechanized manner.

As in other countries, Greece has seen a growing number of cyberattacks, which have made the implementation of the national cybersecurity program a top priority. Until 2016, Greece has not developed a national cybersecurity strategy [10]. The Greek government has created the National Cyber Security Authority (NCSA) to safeguard the digital transformation of the country from growing cyber threats and implement a national cybersecurity strategy. This strategy defines the objectives, priorities, policy, and regulatory measures needed to secure the public and private sectors and critical infrastructures [11]. The existing national cybersecurity strategy focuses on risk management, emerging technologies, and

security requirements, and it highlights the need for collaboration between the public and private sectors [12].

As technology evolves, businesses face new opportunities and threats in managing their data and other forms of intellectual property. Chief information officers attempt to find technological answers to this problem [13–17]. Therefore, IT managers have come to recognize the significance of information security as a factor that contributes to the long-term viability of business operations. The definition of information security policy rules and strategies is used in the execution of security-related initiatives. In addition, it is a condensed document that identifies the program's aims, information security measures, and risk parameters [18]. The complexity of emerging technologies, external and internal threats, and compliance regulations are just a few of the many factors that impact the development and implementation of an effective information security policy [19].

The goal of information security, according to Hong et al. (2006) [20], is to safeguard individuals' private information and businesses' valuable assets during the design, development, and implementation of associated hardware, software, and data systems. One of the primary goals of an information security strategy is to ensure that security measures are consistent with overall business objectives. Its lifecycle consists of several interrelated but distinct stages, including but not limited to business risk analysis, planning, design, development, deployment, operation, assessment, and enhancement [17]. Accordingly, addressing issues with information security is not just a technical problem; it also involves a wide range of managerial and behavioral considerations. Managers frequently ignore these concerns [17,21].

These factors explain the reasons that country entities across the world have begun to formulate and implement cybersecurity strategies and recognize the safeguarding of cyberspace as a fundamental international issue [2]. The National Cybersecurity Strategy can be considered a tool for governments to improve online security and integrity, ensure the openness and resilience of critical infrastructure, and protect the privacy of exchanged digital information. Furthermore, it determines the basic rules of an open society, constitutional freedoms, and legislative rights [9]. All participating actors, such as public authorities, stakeholders from the private sector, or individual citizens, have to consider the increasing importance of this issue, be responsible for protecting themselves, and, if necessary, ensure a well-organized response to increase the rate of cybersecurity. Member States develop national Network and Information Security (NIS) collaboration plans in order to be activated in the case of cyber threats. These plans clearly determine their roles and responsibilities and optimize response actions [13].

The aim of this study is to provide a model based on the ITU cybersecurity decisions, with the goal of developing a roadmap for the successful development and implementation of the National Cybersecurity Strategy in Greece.

The structure of this article is as follows: A theoretical framework in terms of information security management and strategic planning and the cybersecurity strategy is described in Section 2. In Section 4, the suggested framework is presented. Section 6 presents conclusions, implications, limitations, and suggestions for further research.

2. Theoretical Framework

2.1. Information Security Management and Strategic Planning

Information security policies incorporate business and organizational needs for risk management and cost-benefit analysis. Due to the obvious, ever-changing nature of the threats we face, it is essential that our information security policy be regularly reviewed and updated. As a result, it is crucial that security policy practices and procedures are coordinated and aligned with business operations, and this is exactly what the information security policy does. Strategic planning principles inform the creation of an information security plan by outlining a series of projects that will be carried out in accordance with predetermined business goals. Sub-policies are a part of the information security policy and should be reviewed before being put into action. This method is related to the strategic

planning of business initiatives and resembles the formulation of a business strategy or policy [18,22–24].

Different phases based on information security management and strategic management are present in earlier models that include information security policy and strategic planning. Every framework incorporates steps such as risk analysis, policy creation, information security plan creation, policy implementation, and policy evaluation. Environmental analysis and policy alignment are two steps often skipped over by models.

Flowerday and Tuyikeze (2016) [19] presented a framework named "Information Security Policy Development Life Cycle", which incorporates five stages that are predicated largely on the security policy development, implementation, and evaluation. They do not make any reference to strategic management, environmental analysis, or goal setting. Then, Narain Singh et al. (2014) [17] presented a framework that is concerned with three main aspects of information security: setting goals, assessing needs, and creating safeguards. They do not care about carrying out a long-term strategy for security policy. On the other hand, Corpuz (2011) [18] presented an integrated framework for information security policy called the "Corporate Strategic Management Cycle". However, this framework does not include the definition of security goals because it is based on the process of strategic planning. Each step of this model in the field of information security management is implemented using tools and methods based on strategic planning. According to this point of view, a framework based on the strategic planning process was presented by Abu-Musa (2010) [25]. Market conditions, legislation, regulations, IT opportunities, security threats, and norms and best practices in the industry are just some of the external environments considered in this model. Next, there is a breakdown of the technological landscape and the business culture. Managers are responsible for establishing an overarching vision, establishing objectives, policies, standards, and guidelines for information security, and ensuring that IT and business strategies are aligned. At last, the information security strategy is put into action, followed by an assessment of the security measures in place. To better manage information security, Eloff and Eloff (2005) [26] introduced a cyclical model that incorporates strategic management and information security architecture into its various stages. Table 1 presents a summary of the existing frameworks.

Table 1. Existing frameworks.

Phases of Frameworks	References
Security policy drivers Security policy guidance Risk assessment Policy construction Policy implementation Policy compliance Policy monitoring	[19]
Risk assessment Security baselines IT strategy Regularity requirements External factors Internal factors Information security governance outcomes Security objectives Security policies Security standards Security guidelines Implementation Evaluation	[25]

Table 1. *Cont.*

Phases of Frameworks	References
Plan phase Deliver phase Operate phase Security infrastructure Security policies Risk management	[25]
Environmental scanning Strategy formulation Strategy implementation Strategy evaluation Security policy Risk policy Technology policy	[18]

2.2. Cybersecurity Strategy

A cyberattack could result in blackouts and actions of consecutive failures in other interdependent systems that start a chain of events and impact the country's power grid. Many of these information technology (IT) systems, services, networks, and infrastructures are the foundation for economic and social progress. These technological structures are crucial because they either aid in the manufacturing of goods and services or serve as the foundation for other essential institutions. Malicious activity, in particular, has far-reaching consequences, impacting not only the primary critical infrastructure but also all of the connected systems. In today's digital age, where everything is getting more and more connected, widespread Internet access and availability have made it easier for countries and local communities to work together. There may be connections between some important infrastructures in different countries and other platforms. As a result, a mistake or accident is likely to affect systems and networks in different countries [27–29].

These potential misapplications and incidents provide an explanation for the reasons why countries and entities all over the world have raised the issue of the development and implementation of cybersecurity strategies. The governments and organizations of these countries have agreed that protecting cyberspace is an important international issue [28,30,31]. A national plan for cybersecurity strategy is needed for governments to improve online security, protect the openness and resilience of infrastructure, ensure the integrity of digital information that is exchanged, and protect the privacy of digital information that is exchanged. In addition, it spells out the basic rules that govern an open society, as well as constitutional freedoms and legal rights [32]. Actors, such as public authorities, private sector stakeholders, or individual citizens who join the cybersecurity strategy, have a responsibility to take into account the growing significance of this area, be responsible for their own security, and, if necessary, make sure to create a well-organized reaction to boost cybersecurity. The different Member States have worked together to make plans for National Network and Information Security (NIS) collaboration that are ready to be used if cyber threats happen. The main purpose of these plans is to tell member states what their roles and responsibilities are and to show them how to respond [28,31,33]. Even while governments understand the value of the National Cybersecurity Strategy, there has not been much work conducted to develop a method for evaluating cybersecurity attitudes on a national scale that takes into account the factors and indicators that are unique to each country [29,34].

Modern cybersecurity solutions for companies, which are created to offer multifaceted preemptive security, use problem-solving and threat intellect technologies to identify undisclosed threats, safeguarding a large scope of devices (servers, PCs, mobile devices, etc.) and business activities (BYOD, remote access, utilization of cloud-based applications and services, etc.). Because of this difficulty, no individual security solution can effectively

tackle the entire threat landscape. Threats can range from comparatively safe, offensive content (e.g., spam messages) and other inconsequential opportunistic attacks to extremely damaging (malicious code), while they can increase to targeted attacks (such as spyware, denial of service, etc.), with significant operational and financial costs for the organization. The world's foremost cybersecurity firms, such as Symantec with McAfee (endpoint protection software), Cisco (next-generation firewalls and security program), FireEye (network security gateway and email threat protection), and Alien-Vault (behavioral monitoring program and unified security control) are presently providing solutions designed to meet the needs of small companies. Others, such as F-Secure and LogRhythm (security intelligence and analytics platform), provide customized cybersecurity solutions personalized for small businesses comprising those with no IT staff. Additionally, merchants are providing dedicated security solutions, such as NSFOCUS's hybrid distributed denial of service (DDoS) recognition and reduction (on-premises and cloud), Lookout's mobile and app security solutions, Pertino's secure solution for commercial virtualization (in the cloud) freshly procured by Cradlepoint, Splunk's operational intelligence platform, and Balabit's blind spotter user behavior analytics and log management solution, providing edge routing for mini branch networks. Lastly, large data analytics provide novel opportunities in security handling, while encryption technologies can protect important information and communications. However, both are progressively being employed for this reason by different organizations and security startups in Europe (e.g., Silent Circle with its private-by-design smartphone, ZenMate's software for enterprises, and Darktrace's enterprise immune system). Furthermore, even though programmable logic as a way of fast-tracking applications has been in the limelight of both academia and the industry in recent times, there is a visible absence of holistic attempts to tackle the subject of a programmable logic platform that can be combined into the cloud. Apart from [35–37], only one notable solution, centered on the FPGA system on chip (SoC) platform, was established inside the T-NOVA FP7 project [38].

3. Cybersecurity Strategy in Greece

The European Union's 2013 Cybersecurity Strategy [33] is regarded as its primary strategic document in the area of cybersecurity. Particularly in the European Union, the development and dissemination of national cybersecurity strategies have been clearly seen, and this process has accelerated since 2011. However, many nations still lack such strategies (in some of these countries, the strategies are being developed). Differences at the national level are always a possibility when it comes to national cybersecurity strategies; as a result, the strategies themselves and their substance may differ; nonetheless, common strategy components can be analyzed. The setting for the strategy's implementation is tied to the rise in both purposeful and unintentional cybersecurity incidents, and it has been identified that cybercrime has a negative impact on the EU economy [33].

Since the Greek government intends to boost economic growth as well as the networks and services that are provided in digital markets, both in the public and private sectors, it is necessary for Greece to develop and implement a national cybersecurity strategy. On the other hand, Greece only recently started to work on making a strategy for cybersecurity. The National Cybersecurity Strategy comprises these four fundamental tenets. The first one talks about building a strong and safe cyberspace that follows the rules, standards, and best practices that have been set at the national, EU, and international levels. Therefore, values such as freedom, justice, and openness will be protected in cyberspace, and both public and private stakeholders, as well as citizens, will be able to participate and interact safely. The second principle talks about making sure that the capabilities needed to protect against threats are always getting better and making sure that critical infrastructure is built so that it can be protected. Institutional shielding is a part of the third principle of the national cybersecurity framework. This is part of an effort to make cyberattacks less harmful. The fourth and final principle of the National Cybersecurity Strategy [32] calls for the development of a security culture among citizens and stakeholders in the public and private sectors. This is a very important part of the strategy. However, significant components such

as milestones or performance measures are not incorporated in the National Cybersecurity Strategy. Because of this, it is hard for stakeholders to keep track of the cybersecurity strategic plan to make sure that the goals and objectives are met. Benchmarks should be established in the National Cybersecurity Strategy for achieving concrete outcomes, and they should be affiliated with transparency and implementation along with performance indicators to support in deciding whether progress is being achieved. None of the people involved have a full understanding of the costs and resources, including how to justify the investment that will be needed, which is important for support [32].

The government stresses how important it is to have a clearly defined oversight process so that agencies that are in charge of making effective cybersecurity measures can do so. This is because there are many ongoing cybersecurity problem programs aimed at information security [39]. In addition, the National Cybersecurity Strategy does not make a reference to the implementation of risk assessment analysis at the national level. Hazard analysis research is a fundamental and technological process that is based on the recognition, assessment, and evaluation of the impact of risk, and it contributes to the creation of a plan for the protection of vital infrastructure, networks, or platforms according to the sector and/or the stakeholder. The National Cybersecurity Strategy does not make a reference to the implementation of risk assessment analysis at the national level. The process ought to incorporate all possible dangers and harmful activities in accordance with cyberattacks, in addition to the risks that are linked with natural occurrences, harmful technological malfunctions or breakdowns, and human error. The interdependency of the information systems of the stakeholders who participate in the National Cybersecurity Strategy is the root cause of these threats; consequently, stakeholders ought to conduct additional research into the breadth and depth of the repercussions at the national level [32].

In order to address these challenges, government agencies are tasked with developing and putting into action risk-based federal and critical infrastructure programs. These programs will assist the agencies in identifying and mitigating threats posed by the online environment, as well as responding to and mitigating those threats. Other significant steps that governments can take include raising public awareness about the importance of maintaining a secure presence online, encouraging education and workforce planning, and stepping up their research and development efforts (R&D). Due to the challenges that are currently being faced by federal agencies, it will be difficult to achieve the primary goal of providing support for targeted cyber R&D. In addition, government agencies have the ability to delegate roles and responsibilities associated with international facets of cybersecurity, as well as the ability to collaborate with one another on an international level in order to address challenges associated with international cybersecurity [39,40].

In particular, the knowledge regarding cyber threats could be improved if citizens were informed about cyberattacks and malicious activities in relation to cybersecurity and the social impact of these activities. As a result, educational campaigns aimed at stakeholders from the public and private sectors, as well as citizens who are taking part in the development of the National Cybersecurity Strategy, might be useful. These campaigns have the potential to increase the level of protection against malicious actions, and they also have the potential to increase the level of cybersecurity in Greece [32].

4. Suggested Framework for National Cybersecurity Strategy

In order to accomplish the objectives of the National Strategy, the first phase involves the formulation and execution of a National Strategy as well as an examination of the existing institutional structure. The second phase of the National Strategy should focus on defining the legislation, roles, and competencies of the various stakeholders involved in cybersecurity issues such as the processing of personal data, electronic communications, the waiving of confidentiality of communications, and the availability and integrity of networks. Additionally, the regulatory acts that are specialized for each industry as well as their influence to date on the support of cybersecurity should be specified in the National Strategy document. In addition, the National Cybersecurity Strategy needs to define the structures,

stakeholders, and services of the public or private sector that have a role in the operational protection of cybersecurity. Additionally, current emergency plans should be developed in addition to EU and other international directives and regulations in accordance with network and information security as well as the security of critical infrastructure. In the final phase of the framework, the effectiveness of the current institutional framework is evaluated in order to describe overlaps and points that require improvement and more efficient coordination. This is performed in order to define the points at which more effective coordination is needed [32].

In order to ascertain the frameworks and indices for minimizing cyber risks based on important information and communication systems, it is necessary to construct a National Cyberspace Contingency Plan. Participants include those who have an interest in restoring the services they provide to society as part of the National Cybersecurity Strategy [32].

These features and components should be incorporated into the national strategy so that it can better serve as a guide for resource and government bodies, hold those responsible for its creation to account, and have the greatest possible impact on the national level [39]. It is crucial that the authorities in charge of each country's NIS work together to develop a plan for coordinating prevention, detection, mitigation, and response activities.

Problems arising from worldwide interconnected networks affect individuals, businesses, and authorities. In order to secure network equipment and reduce occurrences, national-level coordination of prevention, response, and recovery efforts is required. Through coordination, government agencies, corporate sector actors, academic institutions, and regional and international organizations will be better able to identify risks and implement solutions. Funding, human resources, technological capabilities, training, collaboration between the public and private sectors, and regulatory requirements are all required for effective incident management [29,40]. Because of the lack of a legal structure [41], Greece finds it difficult to share its cybersecurity assets across borders or with other Member States. Actions that must be taken include the construction of organizational structures at the national and regional levels; the promotion of communications; information dissemination; and the acknowledgment of digital credentials across different countries. However, further activities are needed at the global level, and international cooperation is needed among these many entities [29].

Information exchange between corporate and public sector participants in the National Cybersecurity Strategy and the National Cyber Security Authority is necessary for the successful execution of the National Cybersecurity Strategy, as described above. The private sector can benefit from the open sharing of data about the information and communication systems they manage, the security policies they have developed, and the cyber dangers and security attacks they face. The same can be said for the public sector; information sharing among actors may jeopardize security. This data is essential for determining the severity of incidents related to the state of cybersecurity in the country [32,40]. To reduce events and difficulties related to cyberspace security, businesses and public stakeholders are working together to share knowledge and experience, with the goal of jointly developing appropriate steps to address the problem [31,40].

The proposed framework can be thought of as a fluid model because it incorporates the human, legal, technological, and international relations peculiar to a given country, as well as important principles that might impact the cybersecurity operations of that country. Because stakeholders may learn about the context in which cybersecurity is operating and the tools at their disposal, this framework can be seen as a preventative model that aids national strategists in developing policies and launching initiatives to raise cybersecurity standards.

According to this plan, the federal government will implement significant upgrades to better deal with cybersecurity threats. Agencies with a greater focus on cybersecurity design and implement risk-based programs, reduce and mitigate events, increase research and development activities, promote education and awareness, and plan for and recruit a skilled workforce. Based on the strategy and previous recommendations, agencies

must make a plan to deal with the most important cybersecurity issues. The roadmap should incorporate key elements of the National Cybersecurity Strategy, such as annual evaluations of management, operational, and technical controls; and periodic controls and assessments of the effectiveness of information security policies, practices, and procedures to be implemented based on risk. Additionally, other suggested steps for inclusion in the roadmap creation process are to keep and grow the Member States' scientific, engineering, and market leadership in IT. It is also important to raise public understanding of the cybersecurity risks they face. Supporting organizations and individuals to implement effective actions as they manage risk [39] and training the workforce to secure the country's competitive advantage are two other steps that should be taken into consideration when designing the roadmap.

Lastly, to reach the goal of working with other countries to build an open, interoperable, secure, and reliable information and communications infrastructure [39], it is the job of each government to create and maintain an environment in which laws of responsible behavior guide the actions of nations, keep collaborations going, and support the rule of law in cyberspace.

The framework that has been suggested is based on the institutional framework that already exists, as well as the goals and difficulties outlined in the National Cybersecurity Strategy. It includes the elements that are lacking in the National Cybersecurity Strategy as well as the entities that are involved in the process of developing the National Cybersecurity Strategy. It also involves the desirable qualities of the National Cybersecurity Strategy. Figure 1 provides a presentation of the framework.

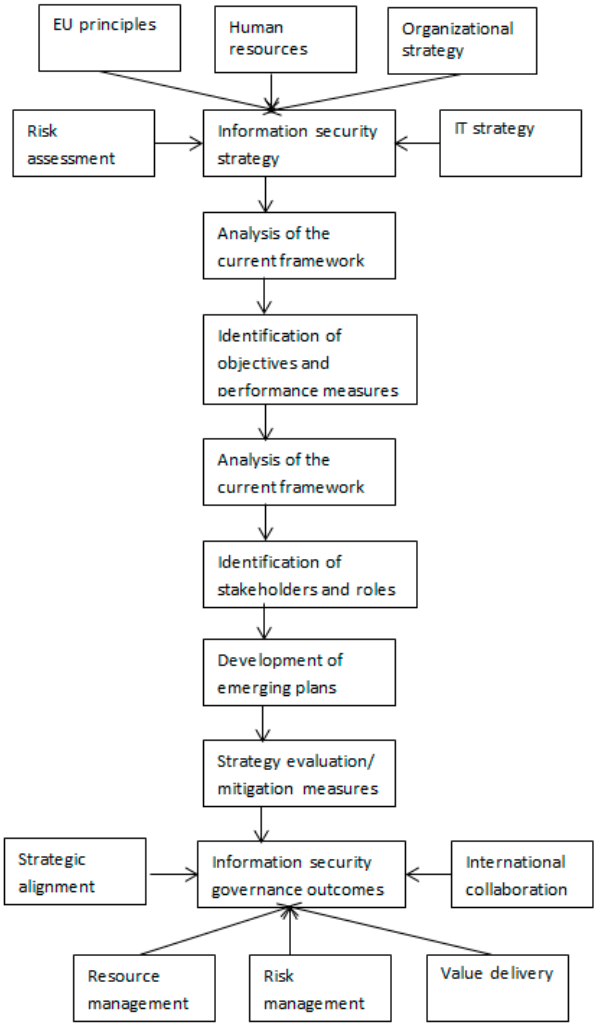

Figure 1. Suggested framework for National Cybersecurity Strategy.

5. Discussion

As a result of globalization, it is essential that cyberspace be safeguarded not only on a national level but also between and across nations. To make sure cybersecurity policies are followed and to lessen or stop the negative effects of possible cyberattacks, agencies in these cultures must create an environment that makes it easy to come up with national strategies and international agreements with other countries [29,31,42].

5.1. Theoretical and Practical Contribution

This paper contributes by providing a model based on the ITU cybersecurity decisions, with the goal of developing a roadmap for the successful development and implementation of the National Cybersecurity Strategy in Greece. This article's main contribution is the creation of a cybersecurity framework. This cybersecurity framework has the potential to pave the way for the creation of a globally applicable and systemic cybersecurity strategy. The development of such a plan will boost a country's capabilities in the areas of cybersecurity, information technology, and innovation. Concurrently, it can help legislators and policymakers craft better laws and design more effective cybersecurity technology, both of which are essential to ensuring that cyberspace operations are secure, effective, and trustworthy. The proposed framework could be put to the test and evaluated by using data on a national level collected by international organizations and appropriate methodologies created for constructing composite indices. The primary focus of Member States at present is on taking a comprehensive approach to cybersecurity. Previous decades have seen governments take a piecemeal approach to cybersecurity.

Some implications can be seen on both the domestic and international levels. At the national level, people with a lot of power in the public and private sectors, such as the top managers, government officials, and academics, work together to come up with ways to reduce attacks. Regarding the worldwide platform, community enterprises from various nations work together to increase awareness of cybersecurity threats and create a universal global awareness that occurrences in cyberspace are highly hazardous, and they come to an agreement not to use them. By signing an agreement against the use of cyberspace, for instance, countries can increase cooperation between their different national intelligence entities and share data about cybercrimes and incidents. Such policies have many advantages, including boosting international cooperation and agreements, strengthening public-private partnerships, raising public awareness, and encouraging human capital to become educated on cybersecurity challenges, work together to develop effective solutions, and divide the burden of preventing cybercrime among all relevant community members.

5.2. Limitations and Suggestions for Future Research

This article has some limitations. An empirical survey to verify conceptual understanding with ground realities has not been conducted on the conceptual framework. The identified organizational factors and the factors related to information security policy, as well as their integration, were only studied in one country. Consequently, recommendations for further study are provided. The world's governments could be given some recommendations for improving cybersecurity and responding to cyberattacks. As part of a larger, more holistic framework, the indicators collected can be used to optimize these initiatives. A country's policymakers, strategists, and economists can use the foregoing implications to inform the development of an analytical model that identifies gaps, incorporates threat assessments, defines vulnerabilities, and develops appropriate responses. This systemic method can be used to develop a complete strategy for dealing with the issue of cyberspace. The outcomes of the cyberattacks the sector has been experiencing, as well as the singularity of the country's assets in terms of critical infrastructures, national security, and economic security, should inform the developed responses.

National stakeholders must develop a comprehensive strategic model to lessen the chances of cyber threats and incidents, as both government agencies and the country's

cyber-critical infrastructure face a growing number of challenges. This strategic method would allow us to pinpoint the most pressing issues and efficiently allocate resources. As an added bonus, a convincing model could be developed to justify expenses; stakeholders' roles and responsibilities could be defined; goals and priorities could be established; and participants who are accountable for achieving the goals could be specified. Although governments have begun to recognize the importance of considering such factors as milestones and performance measures, specific roles and responsibilities of stakeholders, and costs and sources of funding when developing a cybersecurity strategy, this process is still in its infancy. The current strategy does not include priority actions, who is in charge of doing them, or when they should be performed. Because of this, the nation's integrated cybersecurity strategy is still not clear and is not fully formed.

The modeling of cybersecurity strategy assists countries in aligning it with operations and processes to understand better their vision, mission, goals, and culture. Thus, policymakers, through the visualization of the country's cybersecurity strategy, should be aware of its strategy, goals, and structure to effectively use the necessary resources and develop digital tools that help the country digitalize its processes and increase its efficiency. As scholars conclude that strategic planning in enterprise architecture (EA) can improve the traceability between a country's strategic planning and EA choices, and EA can also be used for strategy formulation, the modeling of cybersecurity strategy in EA is a significant step toward this alignment. Without being able to envision what that process looks like, it becomes difficult to fully comprehend what is required for success. Therefore, scholars suggest more practical case studies should be conducted in order to improve the ease of use and clarity of cybersecurity strategy concepts.

6. Conclusions

The aim of this study was to provide a model based on the ITU cybersecurity decisions, with the goal of developing a roadmap for the successful development and implementation of the National Cybersecurity Strategy in Greece. The suggested framework was based on the institutional framework that already exists, as well as the goals and difficulties outlined in the National Cybersecurity Strategy. It included the elements that are lacking in the National Cybersecurity Strategy as well as the entities that are involved in the process of developing the National Cybersecurity Strategy. It also involved the desirable qualities of the National Cybersecurity Strategy.

Author Contributions: Conceptualization, F.K. and M.K.; methodology, F.K.; formal analysis, M.K.; investigation, M.K.; data curation, F.K.; writing—original draft preparation, F.K. and M.K.; writing—review and editing, F.K. and M.K.; supervision, F.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Palvia, P.; Baqir, N.; Nemati, H. ICT for socio-economic development: A citizens' perspective. *Inf. Manag.* **2018**, *55*, 160–176. [CrossRef]
2. Sargent, J.; Ahmed, A. What Is IT for Social Impact?: A Review of Literature and Practices. *IEEE Technol. Soc. Mag.* **2017**, *36*, 62–72. [CrossRef]
3. Xinaris, C. The individual in an ICT world. *Eur. J. Commun.* **2016**, *31*, 58–68. [CrossRef]
4. Cheng, C.-Y.; Chien, M.-S.; Lee, C.-C. ICT diffusion, financial development, and economic growth: An international cross-country analysis. *Econ. Model.* **2021**, *94*, 662–671. [CrossRef]

5. Fernández-Portillo, A.; Almodóvar-González, M.; Coca-Pérez, J.L.; Jiménez-Naranjo, H.V. Is Sustainable Economic Development Possible Thanks to the Deployment of ICT? *Sustainability* **2019**, *11*, 6307. [CrossRef]
6. Evans, O. Information and communication technologies and economic development in Africa in the short and long run. *Int. J. Technol. Manag. Sustain. Dev.* **2019**, *18*, 127–146. [CrossRef]
7. Naveed, K.; Watanabe, C.; Neittaanmäki, P. The transformative direction of innovation toward an IoT-based society-Increasing dependency on uncaptured GDP in global ICT firms. *Technol. Soc.* **2018**, *53*, 23–46. [CrossRef]
8. Polder, M.; de Bondt, H.; van Leeuwen, G. Business dynamics, industry productivity growth, and the distribution of firm-level performance: Evidence for the role of ICT using Dutch firm-level data. *J. Technol. Transf.* **2018**, *43*, 1522–1541. [CrossRef]
9. Roztocki, N.; Soja, P.; Weistroffer, H.R. The role of information and communication technologies in socioeconomic development: Towards a multi-dimensional framework. *Inf. Technol. Dev.* **2019**, *25*, 171–183. [CrossRef]
10. Wong, C.H.; Ho, W.-C. Roles of social impact assessment practitioners. *Environ. Impact Assess. Rev.* **2015**, *50*, 124–133. [CrossRef]
11. Aledo-Tur, A.; Domínguez-Gómez, J.A. Social Impact Assessment (SIA) from a multidimensional paradigmatic perspective: Challenges and opportunities. *J. Environ. Manag.* **2017**, *195*, 56–61. [CrossRef] [PubMed]
12. Arce-Gomez, A.; Donovan, J.D.; Bedggood, R.E. Social impact assessments: Developing a consolidated conceptual framework. *Environ. Impact Assess. Rev.* **2015**, *50*, 85–94. [CrossRef]
13. Kitsios, F.; Kamariotou, M. Information Systems Strategy and Strategy-as-Practice: Planning Evaluation in SMEs. In Proceedings of the Americas Conference on Information Systems (AMCIS2019), Cancun, Mexico, 15–17 August 2019; pp. 1–10.
14. Kitsios, F.; Kamariotou, M. Decision Support Systems and Strategic Information Systems Planning for Strategy Implementation. In *Strategic Innovative Marketing*; Kavoura, A., Sakas, D., Tomaras, P., Eds.; Springer: Cham, Switzerland, 2017; pp. 327–332.
15. Kitsios, F.; Mitsopoulou, E.; Moustaka, E.; Kamariotou, M. User-Generated Content behavior and digital tourism services: A SEM-neural network model for information trust in social networking sites. *Int. J. Inf. Manag. Data Insights* **2022**, *2*, 100056. [CrossRef]
16. Kitsios, F.; Kamariotou, M.; Karanikolas, P.; Grigoroudis, E. Digital Marketing Platforms and Customer Satisfaction: Identifying eWOM Using Big Data and Text Mining. *Appl. Sci.* **2021**, *11*, 8032. [CrossRef]
17. Singh, A.N.; Gupta, M.P.; Ojha, A. Identifying factors of "organizational information security management". *J. Enterp. Inf. Manag.* **2014**, *27*, 644–667. [CrossRef]
18. Corpuz, M. The enterprise information security policy as a strategic business policy within the corporate strategic plan. In Proceedings of the 15th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, FL, USA, 19–20 July 2011; pp. 275–279.
19. Flowerday, S.V.; Tuyikeze, T. Information security policy development and implementation: The what, how and who. *Comput. Secur.* **2016**, *61*, 169–183. [CrossRef]
20. Hong, K.; Chi, Y.; Chao, L.R.; Tang, J. An empirical study of information security policy on information security elevation in Taiwan. *Inf. Manag. Comput. Secur.* **2006**, *14*, 104–115. [CrossRef]
21. Chatzipoulidis, A.; Mavridis, I. An ICT security management framework. In Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT), Athens, Greece, 26–28 July 2010; pp. 1–4.
22. Kamariotou, M.; Kitsios, F. Critical Factors of Strategic Information Systems Planning Phases in SMEs. In *European, Mediterranean, and Middle Eastern Conference on Information Systems*; Themistocleous, M., Rupino da Cunha, P., Eds.; Springer: Cham, Switzerland, 2019; pp. 503–517.
23. Kitsios, F.; Kamariotou, M. Open Data and high-tech startups: Towards nascent entrepreneurship strategies. In *Encyclopedia of Information Science and Technology*, 4th ed.; IGI Global: Hershey, PA, USA, 2019; pp. 3032–3041.
24. Kitsios, F.; Kamariotou, M. Critical success factors in service innovation strategies: An annotated bibliography on NSD. In Proceedings of the British Academy of Management (BAM) Conference 2016, Newcastle, UK, 6–8 September 2016; pp. 1–28.
25. Abu-Musa, A. Information security governance in Saudi organizations: An empirical study. *Inf. Manag. Comput. Secur.* **2010**, *18*, 226–276. [CrossRef]
26. Eloff, J.; Eloff, M. Information security architecture. *Comput. Fraud. Secur.* **2005**, *2005*, 10–16. [CrossRef]
27. Allianz Risk Barometer. Top Business Risks. 2015. Available online: https://cottrillresearch.com/allianz-risk-barometer-top-global-business/ (accessed on 10 December 2022).
28. Bauer, J.M.; Dutton, W.H. The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet. World Development Report. 2016. Available online: http://documents.worldbank.org/curated/en/689851467991972707/pdf/102965-WP-Box394845B-PUBLIC-WDR16-BP-The-New-Cybersecurity-Agenda-Bauer-Dutton.pdf (accessed on 10 December 2022).
29. Koong, K.; Yunis, M. A Conceptual Model for the Development of A National Cybersecurity Index: An Integrated Framework. In Proceedings of the Twenty-First Americas Conference on Information Systems, Fajardo, Puerto Rico, 13–15 August 2015; pp. 1–13.
30. van Vuuren, J.J.; Leenen, L.; Zaaiman, J. Using an ontology as a model for the implementation of the national cybersecurity policy framework for South Africa. In Proceedings of the ICCWS2014-9th International Conference on Cyber Warfare and Security: ICCWS 2014, West Lafayette, IN, USA, 24–25 March 2014; pp. 107–115.
31. Greek CyberCrime Center. Policy Recommendations for Cyber Security. 2015. Available online: http://www.cybercc.gr/m/GCC_POLICY_RECOMMENDATIONS_FOR_CYBER_SECURITY.pdf (accessed on 10 December 2022).

32. ENISA. Greek National Cyber Security Strategy-Interactive Map. 2017. Available online: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view (accessed on 10 December 2022).
33. European Commission. Joint Communication to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions. Cybersecurity Strategy of The European Union: An Open, Safe and Secure Cyberspace. 2013. Available online: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed on 10 December 2022).
34. Symantec. Internet Security Threat Report. Volume 21. Available online: https://www.phishingbox.com/assets/files/Page_Editor_Files/istr-21-2016-en.pdf (accessed on 10 December 2022).
35. Byma, S.; Steffan, J.G.; Bannazadeh, H.; Garcia, A.L.; Chow, P. Fpgas in the cloud: Booting virtualized hardware accelerators with openstack. In Proceeding of the 2014 IEEE 22nd Annual International Symposium on Field-Programmable Custom Computing Machines, Boston, MA, USA, 11–13 May 2014; pp. 109–116.
36. Fahmy, S.A.; Vipin, K.; Shreejith, S. Virtualized FPGA accelerators for efficient cloud computing. In Proceedings of the 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), Porto, Portugal, 24–26 April 2017; pp. 430–435.
37. Xu, L.; Shi, W.; Suh, T. PFC: Privacy preserving FPGA cloud-a case study of MapReduce. In Proceedings of the 2014 IEEE 7th International Conference on Cloud Computing, Anchorage, Alaska, 27 June–2 July 2014; pp. 280–287.
38. Yeh, T.; Yu, S. Realizing dynamic resource orchestration on cloud systems in the cloud-to-edge continuum. *J. Parallel Distrib. Comput.* **2022**, *160*, 100–109. [CrossRef]
39. GAO. Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. 2013. Available online: https://www.gao.gov/assets/660/652170.pdf (accessed on 10 December 2022).
40. OECD. Cybersecurity Policy Making at A Turning Point: Analysing A New Generation of National Cybersecurity Strategies for The Internet Economy. 2012. Available online: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf (accessed on 10 December 2022).
41. ITU. Cyberwellness Profile Greece. 2015. Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Greece.pdf (accessed on 10 December 2022).
42. Štitilis, D.; Pakutinskas, P.; Malinauskaitė, I. EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Secur. J.* **2017**, *30*, 1151–1168. [CrossRef]