sustainability

Article

Systematically Understanding Cybersecurity Economics: A Survey

Mazaher Kianpour *, Stewart J. Kowalski and Harald Øverby

Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU Norwegian University of Science and Technology, 2815 Gjøvik, Norway; stewart.kowalski@ntnu.no (S.J.K.); haraldov@ntnu.no (H.Ø.)

* Correspondence: mazaher.kianpour@ntnu.no

Abstract: Insights in the field of cybersecurity economics empower decision makers to make informed decisions that improve their evaluation and management of situations that may lead to catastrophic consequences and threaten the sustainability of digital ecosystems. By drawing on these insights, cybersecurity practitioners have been able to respond to many complex problems that have emerged within the context of cybersecurity over the last two decades. The academic field of cybersecurity economics is highly interdisciplinary since it combines core findings and tools from disciplines such as sociology, psychology, law, political science, and computer science. This study aims to develop an extensive and consistent survey based on a literature review and publicly available reports. This review contributes by aggregating the available knowledge from 28 studies, out of a collection of 628 scholarly articles, to answer five specific research questions. The focus is how identified topics have been conceptualized and studied variously. This review shows that most of the cybersecurity economics models are transitioning from unrealistic, unverifiable, or highly simplified fundamental premises toward dynamic, stochastic, and generalizable models.

Keywords: cybersecurity economics; economics of information security; complex systems; socio-technical systems; meta-narrative literature review; sustainable digital ecosystems

Citation: Kianpour, M.; Kowalski, S.J.; Øverby, H. Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability* **2021**, *13*, 13677. https://doi.org/10.3390/su132413677

Academic Editor: Bruce Morley

Received: 26 October 2021
Accepted: 4 December 2021
Published: 10 December 2021

1. Introduction

At the time of conducting this research, the world is being shaken by an unprecedented upheaval as the coronavirus pandemic has affected billions of people worldwide. This large-scale event has not only affected us in the physical dimension but also cyberspace. Elections, Olympic games, and wars quickly make their way into the cyber world, and adversaries can take advantage of these global incidents to attack people, organizations, and governments. These events have given the decision makers in the cybersecurity domain a pause for reflection. Moreover, the scholars focused on cybersecurity economics are trying to build a consensus on the need to have secure, sustainable hyper-connected digital societies through greater awareness, strong multi-stakeholder partnerships, and deep structural changes in key areas of institutional activities.

The importance of cybersecurity in digital ecosystems has resulted in a large stream of research that focuses on technical defenses and solutions, such as encryption, intrusion prevention systems, and access controls. In addition to the technical defenses, the sustainability of digital ecosystems is at least as much dependent on the aspects that can be explained more clearly and convincingly using the language of economics. However, research focusing on the economic aspects of cybersecurity is at an infant stage, despite four decades of research activity that was started in 1982 by Courtney [1]. He stated that a security control should not be implemented if it costs more than tolerating the problem. He also added that the selection of security controls requires a systematic approach with full recognition of interdependencies and cost–benefit relationships. The economic implications of decisions made in the context of cybersecurity are influenced by the presence of reinforcing features, such as complexity, deep uncertainty, and non-ergodicity.

The economic models with a neoclassical theoretical basis were among the most often used tools in the early stages of cybersecurity economics research. This school of thought imposes a set of assumptions on economics models, including rationality, representative agents, constant returns to scale, and cleared markets in the long-term [2]. However, as the maturity of the field increases, cybersecurity economics literature revealed models which are characterized by dynamic (i.e., accounting time), stochastic (i.e., representing random behavior of agents), and generalizable (i.e., describing the entire ecosystem) features. These models attempt to avoid the oversimplifying assumptions such as homogeneous agents, rationality, and optimizing behavior. Hence, they introduce additional variables to consider bounded rationality, uncertainty, or imperfect information. While a detailed discussion of this school and other schools is beyond this article's scope, we will discuss briefly how they have been applied for cybersecurity economics in Section 3.

This study provides a meta-narrative literature review of existing cybersecurity economics models applicable for cybersecurity investments, information sharing, sustainability, and cyber insurance. Our overall assessment of the literature is critical. The literature has succeeded in providing broad and intriguing coverage of the application of economic analysis to cybersecurity. It presents significant results consistent with complex systems and suggests the presence of the sorts of heterogeneity and interdependencies across agents. It also contributes to developing key competencies (e.g., system thinking, adversarial thinking, and anticipatory competencies) to advance security and sustainability in digital ecosystems. Yet, "The Global Risks Report 2021", published by the World Economic Forum, has categorized cybersecurity failures as clear and present dangers [3]. This category reveals concerns about lives and livelihoods. Moreover, a report by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, shows that in 2020, it was initially forecast that the investment in cybersecurity by the organizations would surpass USD 145 billion [4]. However, despite increasing cybersecurity spending, the annual cost of cybercrime, globally in 2020, is estimated at USD 1 trillion [4], and data breaches continue to proliferate [5]. Now, the question that arises here is whether these models have been effective in developing secure and sustainable digital ecosystems.

These numbers cast doubt over these models' effectiveness, particularly when they compare it with other areas of business investment and performance improvement. For example, the proposed models for cybersecurity investment, as one of the core issues in cybersecurity economics, mainly have limitations such as inaccurate estimates and applying complexity in real-world situations. Limited scenarios and inconsideration of constraints, type of organizations, and adversaries' strategies are common problems of the models that claim accuracy and simplicity. Therefore, our criticism is not that scholars fail to employ models according to the assumptions of particular rationality or perfect markets. Rather, they do not use models adequately and appropriately with respect to the purposefulness of individual behavior and systems' complexity. The limitations of the literature are not surprising given the novelty of cybersecurity economics as an interdisciplinary field. We believe that this field will experience an exploratory and dialectical empirical development. This process is critical for developing economically viable cybersecurity strategies and policies.

In the form of a literature review, this study critically reflects on the literature to build a deep understanding of cybersecurity economics and identify seven core issues that have been subject to analysis under this field. The first contribution of this study is the provision of different schools of economics employed in cybersecurity. The second contribution is presenting (1) the topics and challenges that have been investigated under the perspective of cybersecurity economics, (2) the characteristics of an efficient cybersecurity economic model, and (3) how this field has contributed to providing solutions to known and unknown problems within the cybersecurity domain. Finally, the third contribution is to demonstrate how particular research in economic aspects of cybersecurity has unfolded over time and shaped the kind of questions being asked and the methods used to answer them.

The remainder of this paper is organized as follows. In Section 2, we provide a brief background on the cybersecurity economics. Section 3 presents the theoretical underpinnings of cybersecurity economics models and the schools of thought employed to develop these models. The core issues of cybersecurity economics models are discussed in Section 4. The research methodology of this review is demonstrated in Section 5. The research questions are answered in Section 6. Section 7 concludes by summarizing the key findings of this article and provides insights for future research.

2. Background

The subject of this study is cybersecurity economics. Accordingly, a fundamental issue it must address is what makes cybersecurity economics a single subject of investigation. Indeed, cybersecurity and economics each constitute distinct types of investigation, as reflected in the fact that they have long been studied as two separate disciplines by two large independent groups of researchers, respectively, information and computer scientists and economists. Therefore, there might be barriers to understanding how together they constitute a single field of study. It can be argued that cybersecurity economics should be understood as an interdisciplinary field of study that falls between and combines cybersecurity and economics. However, this perspective faces the problem that there is more than one conception of how different disciplines are related.

Cat [6] presented a taxonomy of possible conceptions: interdisciplinary, multidisciplinary, cross-disciplinary, and transdisciplinary. The strategy adopted in this review is closest to the transdisciplinarity (i.e., a synthetic creation that encompasses work from different disciplines), which treats cybersecurity and economics as two different relatively independent systems of thinking that interact in a complex socio-technical system. A complex socio-technical system paradigm takes the interaction of different systems as the starting point and explains their relative interdependence regarding how they interact in social and technical settings. This paradigm enables us to capture the transformative effects that cybersecurity and economics might each have on one another. To develop a more clear understanding of these effects, this section continues to elaborate on how cybersecurity started to draw from economics.

The terms cybersecurity and information security are often used interchangeably. Solms and Niekerk argue that, despite the substantial overlap between cybersecurity and information security, the two concepts are not equal [7]. They posit that cybersecurity goes beyond traditional information security boundaries to include protecting information resources and other assets, including the human and cyber-physical systems. According to this viewpoint, which is also supported by the international standard ISO/IEC 27032:2012(E), in information security, a reference to the human factor usually relates to humans' role(s) in the security process. In cybersecurity, however, this factor has an additional dimension, namely the humans as potential targets of cyber attacks or even the humans that unknowingly participate in a cyber attack due to lack of awareness.

While ENISA concludes that there does not need to be a definition for cybersecurity [8], we provide a definition to avoid vagueness regarding what cybersecurity entails. Cybersecurity is basically the name of standard practices that involve the people, processes, and technologies in an organization, in a group, or stand-alone environments in which the computers and cyber-physical systems with valuable data are connected to cyberspace. Cybersecurity deals with the different procedures that create a secure environment by protecting the assets. According to ISO/IEC 27002, an asset is anything that has value to an organization [9]. Assets can be categorized into different subtypes based on their convertibility (current and non-current assets), physical existence (tangible or intangible assets), and usage (operating or non-operating assets) [10]. Some assets are relation specific. These assets are the results of one or both parties having made investments to support a particular relationship [11]. For example, people who work for a specific organization and learn skills that are valuable only for that specific organization are considered relation-specific assets. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization.

Valuation of these assets and the risks of loss or damage have been controversial topics in cyber risk management and cybersecurity economics. The valuation methods vary based on cost [12], market [13], and utility [14] of the assets. With the rapid development of information technology, digital assets have been recognized as critical parts of organizations. However, cybersecurity is not limited to digital assets. In the last decade, the increasing number of cyber attacks against physical assets and critical infrastructures (e.g., Stuxnet, Industroyer, Triton, etc.) has indicated that cybersecurity can be labeled as a serious cyber and physical challenge for organizations and governments.

An accurate valuation of assets is central to efficient investment in protecting them, capital budgeting, and strategic planning. This is why this process is changed if poor decisions have been and/or are being made. Much of the published research on cybersecurity economics has been focused on the economic valuation of the assets and finding the optimal security investment level in organizations to protect those assets [15–21]. However, cybersecurity economics not only is concerned with whether an organization is spending enough to secure their assets and whether the security budget is spent on the right security measures and controls [22,23], but is also concerned with how a digital ecosystem and its operating agents function and behave. Cybersecurity economics covers the regulatory changes and competitive pressures (e.g., how cybersecurity can be aligned with broader business processes [24]). It studies how resource allocation by governments and businesses satisfies the requirements of creating a resilient cyber environment for themselves and other agents [25]. Furthermore, cybersecurity economics focuses on the efficiency surrounding the decisions made as a result of incentives and policies that are designed to maximize the profit and trust within the environment [26].

Currently, there is no consensus on a definition of the term cybersecurity economics. Multiple studies have created their definitions, most of which are broad. Probably the most accepted definition for cybersecurity economics is an area concerned with providing maximum protection of assets at the minimum cost [27,28]. However, Rathod and Hämäläinen adopted a wider perspective to the economics of cybersecurity based on strategic, long-term thinking incorporating economics from the outset [26]. They stated that cybersecurity economics and analysis provide benchmarks for the economic assessment of national and international cybersecurity audits and standards. It also provides policy recommendations to align policies and regulations to ensure trust within a digital environment. Additionally, Ahmed argues that cybersecurity economics addresses the issues of protection of Information and Communications Technology (ICT) applications designed to facilitate the economic activities that normally face cybercrimes that cost the companies and countries a significant amount of money and disturb the economic and financial activities around the globe, as has been indicated in ICT-based sustainable development [25].

Despite the many different definitions of cybersecurity economics, all of these studies point out that cybersecurity economic situations are characterized by direct and indirect interdependencies among the agents involved. Each agent's behavior affects the available options of other agents and even the results that they can achieve. Given a particular situation and different options, which option do agents choose and why? Does the outcome satisfy them? Does it unintentionally leave other agents worse off while it has been an optimal decision for some of them? To answer these questions, we would imply that it is crucial to be aware that cybersecurity economics covers a broader range of situations than exchanging products and services for money. Rather, this field of study includes organizations having to decide how to value their assets and scarce resources and adapt economic theories to practice in complex, uncertain environments.

Cybersecurity economics studies include forces motivating stakeholders to invest in cybersecurity provision; market structures and regulatory structures; and environmental, institutional, and distributional consequences of the social decision situation. The studies also investigate the cybercrime economics and motivation, tools, and interest of actors in today's underground marketplaces. All in all, this paper defines cybersecurity economics as a field of research that offers a socio-technical perspective on economic aspects of cybersecurity, such as budgeting, information asymmetry, governance, and types of goods, to provide sustainable policy recommendations, regulatory options, and practical solutions that can substantially improve the cybersecurity posture of the interacting agents in the open socio-technical systems. A socio-technical perspective is essential for understanding and managing the state of cybersecurity today, as well as how to enhance it moving forward.

3. Theoretical Underpinnings of Cybersecurity Economics Models

Colander defines economics as the study of how human beings coordinate their wants and desires, given the decision-making mechanisms, social customs, and political realities of the society [29]. In this definition, the term coordination can mean many things. In our study of cybersecurity economics, we refer to coordination as the efforts to solve problems such as:

- What is the adequate level of cybersecurity and how much should we spend to provide this level.
- How and for whom to provide cybersecurity.
- Who needs to pay for interdependent and cascaded risks.

The answers to these questions, under the assumptions that agents have unlimited resources and complete information, operate in closed systems, and make rational choices, might be clear and straightforward. However, these assumptions are subject to criticism since they rely on unrealistic, unverifiable, or highly simplified fundamental premises. Furthermore, scarcity, incertitude, and ever-changing digital ecosystems make these questions complicated. Hence, understanding the interrelationships among them is central to dealing with the problems mentioned above. Scarcity means that the available resources to satisfy individuals' desires are too few. For example, organizations are faced with a shortage of skilled cybersecurity staff. By 2022, the global cybersecurity workforce shortage is projected to reach upwards of 1.8 million unfilled positions [30].

Moreover, laboratory studies in psychology indicate that attention is also a limited resource [31,32]. In given situations, individuals selectively concentrate on some information while ignoring other perceivable information. These situations embody two main elements: our desires and the resources to fulfill those desires. In the context of cybersecurity, these desires are constantly changing, developing, and partially determined by both society and technological advances. Moreover, the resources and means we employ to fulfill desires can affect those desires. Hence, the degree of scarcity is continually changing and subject to incertitude. Sterling introduced the concept of incertitude to distinguish between uncertainty and risk [33]. According to Figure 1, there are four ways of conceptualizing incertitude. *Risk* refers to situations in which there is moderate knowledge about calculating probabilities for different outcomes. *Ambiguity* differs from risk in the poorly defined characterization of outcomes. Further, *uncertainty* refers to a situation in which outcomes are known, but there is a poor basis for assigning probabilities to these outcomes. Finally, *ignorance* is a situation that combines poor knowledge about both outcomes and likelihood (i.e., a case of surprises).

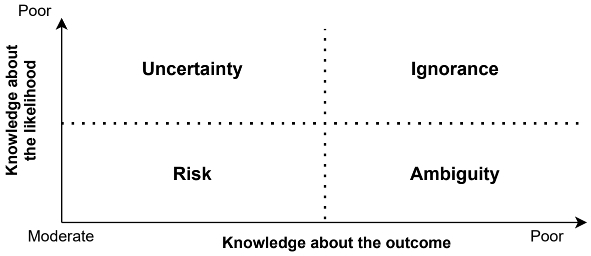

Figure 1. Types of incertitude. Adapted from [33].

When faced with scarcity, we need to make decisions. Decisions are made by comparing the costs and benefits of choices. Rational decision makers invest in cybersecurity if that investment yields a positive return or the marginal cost is less than that of the risk it eliminates. The proposed cybersecurity investment model by Gordon and Loeb [27], and introductory sequence of models based on it [34–36], premised a rational approach to managing risks and making decisions. Nevertheless, is this idealized conception also applicable in real-world situations? Real-world problems require reasoning about distributions over many different internal (e.g., decision-making mechanism, cognitive processes, emotional arousal, etc.) and external factors (e.g., business information, operating environment, available resources, etc.). During the last two decades, various economic models have been constructed to make inferences within cybersecurity by considering these factors. These models are based on generalizations and insights, called theories, about the workings of the cybersecurity market as well as on contextual knowledge about the institutional structure of the interacting stakeholders [37]. This knowledge is acquired from various resources such as individuals, groups, institutions, and systems. Figure 2 depicts that, according to the source of knowledge, economic theories are divided into two branches: microeconomics and macroeconomics.

Microeconomics is the study of individual choice and how economic forces influence that choice [29]. However, to analyze the entire economy built up from microeconomics analysis, everything becomes rather complicated. Therefore, to simplify matters by taking a different approach, macroeconomics studies the economy as a whole. In highly interconnected digital ecosystems, these two branches are very much interrelated. What happens in these environments as a whole is based on individual decisions, but individual decisions are made within an environment and can be understood only within their macro context. Research by Gartner shows that 60% of organizations are now working with more than 1000 third parties [38]. The increasing reliance on partners, sub-contractors, and suppliers contributes to the growing complexity of digital ecosystems and requires an understanding of both micro- and macroeconomics analyses.

Figure 2 shows the particular schools of economic thoughts employed in the cybersecurity economics literature. As the figure shows, some of the schools acquire their knowledge from different resources. Moreover, the problems that matter when looking at the situations from a particular school's perspective are depicted in this figure. It is beyond the scope of this paper to provide a full explanation of these schools. Yet, it is important we reflect on them to understand their characteristics.

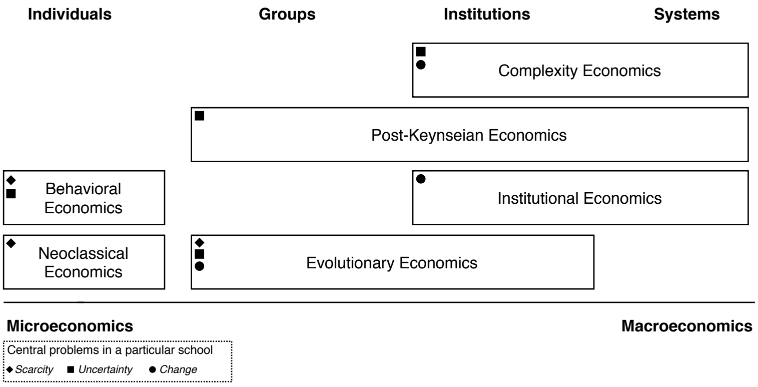
Individuals
Groups
Institutions
Systems
■ ● Complexity Economics
■ Post-Keynseian Economics
◆ ■ Behavioral Economics
● Institutional Economics
◆ Neoclassical Economics
◆ ■ ● Evolutionary Economics
Microeconomics
Macroeconomics
Central problems in a particular school
◆ Scarcity ■ Uncertainty ● Change

Figure 2. The required knowledge in cybersecurity economics model acquired from different resources such as individuals, groups, institutions, and systems. Source: compiled by the authors.

Neoclassical economics forms today's economic mainstream. Organization and allocation of scarce resources is the central economic problem from the neoclassical perspective. It implies that efficiency (i.e., the optimal usage of the available resources to maximize individual utility) is the most relevant evaluation criterion. Econometrics serves as an analytical tool. Mathematical models are used in the analysis of the economic system. It has been argued that rationality, selfishness, and equilibrium are fundamental to neoclassical economics [39]. These paradigmatic cores have been applied in cybersecurity economics by employing two different approaches: decision-theoretic and game-theoretic.

The decision-theoretic approach utilizes traditional risk assessment models to analyze organizations' spending on cybersecurity. Cavusoglu knows these methods are incomplete because of the security problem's strategic nature [40]. Several empirical studies support that attackers do not randomly select their targets and their attack strategies [41–43]. Hence, researchers proposed game-theoretic approaches that treat cybersecurity investment as a game between organizations and attackers [34,40]—or interdependent organizations [44,45]. Aligned with neoclassical economics, the ideal goal of these models is utility maximization. However, this is not the only goal in cybersecurity. In practice, cybersecurity decision makers need to seek how they can mitigate cyber risks, balance business needs and cybersecurity requirements, maintain compliance, and ensure cultural fit [46]. Moreover, the benefits and costs cannot be reliably calculated for cybersecurity since the value of cybersecurity investment comes from the avoidance of potential incidents and the loss reduction from an investment [47,48].

Considering that utility maximization is not the only goal in cybersecurity, neoclassical economics systematically neglects the complexity of our problems and our bounded set of fundamental capabilities, such as rationality, farsightedness, and influence. These limitations are addressed in other economics schools such as behavioral economics, evolutionary economics, and complexity economics. Behavioral economics takes up some of the neoclassical economics critiques by focusing on which decisions are made and what motivations lead to particular actions (in general, observable behavior of humans). In behavioral economics, the findings from psychology, social sciences, neuroscience, and cognitive sciences are transferred to the economic discipline to improve the reliability and precision of explaining human decisions and behaviors [49]. The research on behavioral economics suggests that individuals deviate from the standard model in three respects: *nonstandard preferences* (time preferences, risk preferences, and social preferences), *nonstandard beliefs* (overconfidence, the law of small numbers, and projection bias), and *nonstandard decision making* (framing, limited attention, menu effects, persuasion and social pressure, and emotions) [31].

For example, consider the utility function as a standard model. Individual i at time $t = 0$ maximizes expected utility subject to a probability distribution $p(s)$ of the states of the world $s \in S$:

$$\max_{x_i^t \in X_i} \sum_{t=0}^{\infty} \delta^t \sum_{s_t \in S_t} p(s_t) U(x_i^t | s_t). \tag{1}$$

The utility function $U(x|s)$ is defined over the payoff x_i^t of player i and future utility is discounted with a (time-consistent) discount factor δ. DellaVigna discusses how this function can be deviated from its main hypotheses [31]. The research on nonstandard preferences, beliefs, and decision making constitutes the bulk of the empirical research in psychology and economics. However, some of these topics are relatively new to the field of cybersecurity, and thus there is much that future work can explore. For instance, the results of a study by Kianpour et al. suggest that social preferences have moderating effect on the decision making under cyber risks and uncertainty [37]. With respect to the social preferences, the utility function is $U(x_i, x_{-i}|s)$, meaning that it also depends on the payoff of others x_{-i}. Risk preferences, on the other hand, have been studied more by the researchers under the topics of loss aversion [50,51], insurance [52–54], willingness to pay [55–57], and endowment effect [58,59].

As DellaVigna explains, the standard model in (1) assumes that individuals are normally correct about the distribution of the states $p(s_t)$. However, experiments suggest that they have systematically incorrect beliefs in three ways: overconfidence, the law of small numbers, and projection bias. In the context of cybersecurity, the recent reports show that when it comes to cybersecurity practices, there is general overconfidence among security professionals and C-levels [60]. NIST defines overconfidence as the tendency for stakeholders to be overly optimistic about either the potential benefits of an opportunity or the ability to handle a threat. Dong et al. discussed how overconfidence is negatively associated with information security investment and information security performance in organizations [61].

Nevertheless, incorporating this variable with more complex situations, such as budget constraints and risk interdependencies, could reveal more insights into the role of overconfidence in cybersecurity provision. As with many of the issues raised in this, there is limited literature on projection bias and the law of small numbers and projection bias. However, these issues concern the part of the decision-making process that probabilities need to be considered. Therefore, studying the impact of these beliefs can help us understand why decision makers underestimate cyber risks or underinvest in cybersecurity solutions.

Given the standard utility $U(x|s)$ and belief $p(s)$, individuals may make nonstandard decisions. This can be caused by different framing of a situation, the underweighting (or overweighting) of information because of limited attention, suboptimal heuristics used for choices out of menu sets, social pressure, and emotions. The framing effect is one of the many different cognitive biases that we can be susceptible to. Framing strategies (i.e., strategies for communicating a complex societal problem in such a way that the main arguments are clearly understandable and cannot be easily challenged [62]) have been studied extensively in the context of cyber risk [63–65] and cyber warfare [66,67]. A situation that is framed differently may elicit different responses [68]. Bruijn and Janssen described how evidence-based framing can be used to build cybersecurity awareness. They argue that, in cybersecurity policymaking, utopian or dystopian views might be counterproductive and result in complicating the problems [69]. The findings of another study show how news media framing can generate privacy tradeoffs in exchange for stronger cybersecurity prevention or economic gains [70]. When high societal risks are perceived through news media framing, individuals engage in privacy tradeoffs, encouraging them to comply with intrusive privacy initiatives. Unlike the framing effect, the impact of emotions also has been addressed in cybersecurity decision making. Blunden et al. investigated two threat-induced emotions after a cyber attack: fear and anxiety [71]. Their results show that fearful participants embrace avoidance as their safety behavior, while anxious participants appeal to surveillance and vigilance.

Moreover, Renaud and Dupuis have presented cybersecurity studies that use fear appeals [72]. They outline the literature's limitations and how cybersecurity researchers can study fear appeal models in field experiments rather than laboratory experiments. Many other biases are identified in cognitive psychology. However, unlike framing effects and emotions, other patterns of deviations from standard decision making within the context of cybersecurity are not well-addressed. With the extension of cybersecurity to susceptible areas such as military and critical infrastructures, investigating the impacts of other cognitive biases on people's decisions must be weighed alongside other topics to avoid inference and reasoning problems.

As we mentioned earlier, neoclassical economics ignores the complexity of the problems. Evolutionary economics and complexity economics, on the other hand, use computational and mathematical analysis to explore the complex structures and investigate how and why the systems change. These schools look at the evolutionary systems, not the systems continuously in or tending toward equilibrium. This emphasis on the changing nature of the systems appears to be the crucial feature within the context of cybersecurity. Cybersecurity is no longer a barrier to change [73]. Instead, it is considered as a business enabler or an influencer [74]. Consequently, topics including structural and technological changes, innovation processes, and capabilities development could be used in this domain to explain both change and stability. It should be noted that neoclassical economics can also incorporate dynamic elements such as path dependencies [75]. However, evolutionary economics deals with uncertainty and change in addition to the optimal usage of scarce resources to satisfy individual needs. Therefore, both knowledge and individuals are considered crucial phenomena. Methodologically, evolutionary economics assumes that agents' interaction leads to the formation of new entities and causes of a phenomenon known as emergence. These entities' characteristics cannot be reduced to the individual level, and the performance of the system is determined by the practical level of available knowledge shared among the individuals.

Shiozawa has identified a non-exclusive and non-comprehensive list of seven economic entities being subject to evolutionary changes: economic behavior, commodities, technology, institutions, organizations, systems, and knowledge [76]. While a decision of an individual can change economic behavior, institutions require broad social support to change. For example, the internet is a new system that has quickly become an institution. The present form of this system evolves autonomously, and no one can completely control it, albeit its basic concepts are the results of human design. This category shows that evolutionary economics is compatible with other schools of thought such as behavioral economics, institutional economics, and complexity economics. However, they are different in their perspective, fundamental assumptions, independence of context, etc.

These schools, known as Heterodox economics, have been applied within the context of cybersecurity using different methods such as evolutionary game theory, behavioral game theory, simulation, agent-based modeling, and system dynamics modeling. Different works have relied on the certain concepts of these schools to provide detailed descriptions and arguments grounded in economics about different aspects of cybersecurity and cyberspace. For example, drawing from institutional economics, Kuerbis and Badiei presented a conceptual model to describe the cybersecurity governance landscape based on three governance structures that are commonly noted in institutional economics: markets, hierarchies, and networks [77]. Lindsay has also combined concepts from international relations theory and new institutional economics to understand cyberspace as a complex global institution with contracts embodied in both software code and human practice [78]. He argues that constitutive inefficiencies (market and regulatory failure) and incomplete contracts (generative features and unintended flaws) create the vulnerabilities that hackers exploit and increase the likelihood and magnitude of cyber conflicts.

4. Cybersecurity Economics Models: Core Issues

In 2001, Anderson [79] asserted that providing security of information assets is more than focusing on technological risks. He added that the management of information security is a much deeper problem that has to be explained more clearly and convincingly using the language of economics. Since then, various attempts were made to provide intelligence for cybersecurity decision makers and assess the cyberspace environment using economic models. Most of these models use "Security Level" as an aggregated economic variable to determine the efficiency of the models [80]. However, Böhme and Nowey outlined the economic metrics of security, including annual loss expectancy (ALE), the expected net benefit of investment in information security (ENBIS), the expected benefit of investment in information security (EBIS), and return on security investment (ROSI). Some of the models also defined new metrics to cover more details in their proposed models. For example, References [27,81] defined the security breach probability function, which maps the monetary value of the investment in security and the probability of incurring a pre-defined loss. These metrics enable us to compare the proposed solutions to budgeting problems (e.g., investment, externalities, and insurance). However, budgeting is not the only core issue of cybersecurity economics. In this section, we highlight issues such as economic efficiency, interdependent risks, information asymmetry, and governance.

The analysis of investment models and suggestions of new models have attracted quite a lot of interest in the economics of cybersecurity. The security investment models are used to determine the optimal level of security investments to reduce security risks in the organization effectively. This line of research was preceded by Gordon and Loeb, in which an organization's optimal amount to invest in cybersecurity activities was studied [27]. They presented the importance of understanding risks involved in the investment in cybersecurity in order to assess the expected benefit of the investment. The Gordon and Loeb model examines how the firm's optimal level of cybersecurity expenditures varies with the probability that a cyber attack will be successful in the absence of any cybersecurity expenditures and the expected loss to the organization if the attack is successful. A number of researchers have conducted research in order to analyze and extend this model [81–84]. There are also a number of studies that suggested new models to determine the optimal spending on cybersecurity activities or adoption of new secure technologies (e.g., fog computing [85]). Table 1 shows our categorization of some of these models, which have drawn attention by academic and practitioner literature.

Table 1. Cybersecurity investment models.

Approaches	Description	Works
Microeconomics	Game Theory	[16,19,86,87]
	Behavioral Economics	[88,89]
	Combinatorial Approach	[90]
Financial Analysis	Return on Security Investment (ROSI)	[44,91–93]
	Net Present Value (NPV)	[94,95]
	Internal Rate Return (IRR)	[96]
	Combinatorial Approach	[97]
Management Approaches	Decision Theory	[17,98]
	Risk Management	[36,99,100]
	Organization Theories	[101]
	Combinatorial Approach	[102]
Combinatorial Approaches	Management and Microeconomics	[18,27,35,103]
	Management and Financial Analysis	[97]

As this table shows, researchers have employed different approaches to build cybersecurity investment models. One of the most popular methods is game theory. Game theory is a tool to analyze the structure that lies beneath the social interaction, its possibilities and opportunities, the development paths of interactions, and less likely and more likely outcomes [104]. The financial analysis utilizes organization's information from the most recently available years of accounts. This approach is becoming more popular as the impact of cyber incidents on equity market volatility across publicly traded corporations is increasing [105]. For example, a study by Szubartowicz and Schryen indicates that after fundamental security incidents in a given industry, the stock price will react more positively to an organization's announcement of actual cybersecurity investments in comparison to announcements of the intention to invest [106]. Overall, they also found that the lowest abnormal return can be expected when the intention to invest is announced before a fundamental cybersecurity incident and the highest return when actually investing after a fundamental cybersecurity incident in the respective industry.

Management approaches in constructing cybersecurity models have drawn increasing attention because cybersecurity now has a high priority among managers, policymakers, regulators, and enforcement officials across various sectors. Tisdale knows cybersecurity is a knowledge management problem due to the amount of data, perishability of data, technology turnover, and the multitude of stakeholders and information involved [107]. Therefore, methods such as business intelligence [108] and big data analytics [109] can assist managers to find new solutions to emerging problems in this field. This table also shows several models that employed combinatorial approaches, both inter- and intra-category. These approaches allow the models to be flexible and adaptable as they cover more details, such as interdependent security and human expectations. For example, Reference [102] leverages the economics models of [27,35] and applies the expected utility theory and the presented approach in [41] to understand how cybersecurity investments change breach probabilities and potential loss.

In addition to the investment in cybersecurity, externalities and cyber insurance have been rapidly developing topics in cybersecurity economics. Anderson and Moor [110] have borrowed this term from economics to describe the side effects of security operations and transactions. Externalities can be positive (e.g., scientific research and development) or negative (e.g., cybercrimes or security weaknesses). A different set of externalities can be found when we analyze stakeholders' decisions and operations made within the context of cybersecurity. Varian proposed a model to examine whether the defense depends on the sum of the individuals' efforts, or the minimum effort by the free-riders, or the maximum effort by some of the defenders [111]. This is an important challenge if cybersecurity is treated as a public good and poses a problem known as the tragedy of the commons [79]. This category shows that cybersecurity economics includes aspects of leadership, and societal and corporate culture, and encompasses larger economic and sociopolitical elements such as national and international security.

Although measuring the effectiveness of the investment in cybersecurity plays a vital role in decision making, the economics of cybersecurity has other considerable aspects that we need to investigate as well. Hausken [112] emphasizes the importance for the organizations to understand how they can make the most efficient outcome of their cybersecurity strategy planning. This requires a wider perspective towards this issue. Economics of cybersecurity studies factors that actors perceive as relevant for cybersecurity decisions and affect actions by individuals, groups, organizations, and governments, in both the cybersecurity market's social and technical components. These factors are externalities [113,114], information asymmetry [86,99], and alignment of incentives [114,115]. Furthermore, Dacus and Yannakogeorgos [116] proposed an incentive framework to motivate cybersecurity stakeholders to devote more effort to secure their environment. They point out that information asymmetry can cause a moral hazard. Moral hazard arises when cybersecurity service providers' priorities do not match the client's (U.S. Federal Government, in this case) priorities and their incentives are not aligned.

The economic impact of regulations and policies to increase organizations' investments in cybersecurity activities is also discussed in [117–119]. Massacci et al. [120] investigated the optimal way to regulate cybersecurity for critical infrastructure operators. They presented a cybersecurity economics model to show that operators will eventually stop investing in cybersecurity, depending on the incentives, and care only about compliance. They compared the effectiveness of rule-based with risk-based regulations on the incentive for the security investment by employing a game-theoretic model. They concluded that rules could apply to less security-mature actors and actors above a certain maturity threshold would be subject to a risk-based regulatory framework. In addition to investment and policies, we identified seven areas pertaining to cybersecurity economics which have been subject to analysis and explored under this field. These areas are discussed in more detail under Research Question 2 in Section 6.

5. Research Methodology

To pursue this paper′s objectives, conceptual, empirical, and analytical articles published in cybersecurity economics research were analyzed. Given that cybersecurity economics research is a highly interdisciplinary research field, a meta-narrative review approach is used [121]. Meta-narrative review is one of the new approaches to qualitative and mixed-method systematic review. This form of review is especially designed for reviewing topics that have been conceptualized and studied variously by different groups of researchers. It can be used to overview a complex topic area, highlighting the relative strength and limitations of the respective research approaches. This does not mean that we need to know everything about every discipline we are using.

We begin to understand how different paradigmatic assumptions shape different disciplines and perspectives we are drawing on. This adaptation enables us to conduct an inquiry-driven literature review rather than discipline driven. It means that the scope is defined by the need of the subject matter, not determined and guided by the parameter of the discipline [122]. Unlike other literature review methods, such as realist reviews, meta-narrative reviews are primarily concerned with how issues were researched rather than synthesizing the findings and so can be considered a form of multi-level configuring mapping rather than synthesis of research findings [123].

The review starts by developing five research questions that the study sets out to answer. Table 2 shows the identified research questions. A set of search terms are selected from these research questions. We then use the different combinations of these search terms to find relevant studies in academic databases. The focus is not to cover every article published on the topic, but rather to provide a review of different studies which enable us to answer the questions in Table 2. Therefore, we applied inclusion, exclusion, and quality assessment criteria on the identified studies and shortlist the most relevant studies. These studies are referred to as selected studies. They are a combination of early articles (when the concept of cybersecurity economics first appeared), the most cited articles, and more recent articles.

Table 2. Research questions.

RQ1	What are the characteristics of an efficient cybersecurity economic model?
RQ2	What challenges have been addressed by proposing the existing economic models?
RQ3	What are the main issues faced by the current cybersecurity economic models?
RQ4	What data is needed to reliably assess the performance of a cybersecurity economic model?
RQ5	How has cybersecurity economics contributed to providing solutions for known and unknown problems within the cybersecurity domain?

As discussed in Section 2, there are controversial arguments in the literature regarding the definitions of "cybersecurity" and "information security". Consequently, we decided to use both keywords as the primary search terms. For the secondary terms, we used keywords such as model, theories, and analysis. Finally, we constructed the search string using "AND" and "OR" Boolean operators to link the search terms. Table 3 shows the list of primary and secondary search terms and the search string. We used the search string to look for relevant studies in five databases, presented in Table 4. Although we did not specify a time range for the search, the oldest finding based on this search string is the Gordon and Loeb model [27] published in 2002 (ACM Library). According to Scopus, this article has been cited by 660 documents, which is the highest number of citations in the list of our findings. Moreover, based on Google Scholar, this article has the highest number of citations (1563 up to date of search) in the field of cybersecurity economics. After the Gordon and Loeb model, "Why information security is hard-an economic perspective" by Ross Anderson [79] has acquired the highest number of citations (Scopus: 357, Google Scholar: 1096) in the field of cybersecurity economics.

Table 4 shows the number of findings using our search string in academic databases. We found that many of the studies were indexed by more than one database. Therefore, to avoid duplicates, we screened the results manually and removed the 73 identical results.

Study Selection

We selected the studies in two phases. In the first phase, we excluded according to the criteria presented in Table 5. Our study is not a Multivocal Literature Review (MLR). MLR is a form of a systematic literature review which includes the grey literature (e.g., blog posts, videos, and white papers) in addition to the published (formal) literature (e.g., journal and conference papers) [124]. After exclusion of the results, 385 studies were selected. Then, we applied the inclusion criteria (see Table 6) to identify the most relevant studies to our research questions. A total of 62 studies passed our inclusion criteria. In the second phase, we applied the quality assessment listed in Table 7 to the studies identified in the first phase. After this assessment, 28 studies were selected.

Table 3. Search terms.

Criteria	Description
Primary Search Terms	cybersecurity economics, information security economics, economics of cybersecurity, economics of information security, cybersecurity investment, cybersecurity spending
Secondary Search Terms	model, theories, framework, analysis
Search String	("cybersecurity economics" OR "information security economics" OR "economics of cybersecurity" OR "economics of information security" OR "cybersecurity investment" OR "cybersecurity spending") AND ("model" OR "theories" OR "framework" OR "analysis")

Table 4. Search results (date: 27 August 2021).

Database	Number of Results
IEEE Xplore	26
SpringerLink	489
ScienceDirect	124
ACM Library	62
Total	701
Total (without duplicates)	628

Table 5. Exclusion criteria (EC).

ID	Description
EC1	Short papers, extended abstracts, and studies that do not provide significant new ideas or insights.
EC2	Gray literature (e.g., blog posts, videos, and white papers).
EC3	Non-English studies.
EC4	The study mainly or exclusively investigates non-economic approaches of cybersecurity (e.g., purely risk management or loss prevention expenses).

Table 6. Inclusion criteria (IC).

ID	Description
IC1	The study describes the theoretical function of the employed economic theories and proposed models.
IC2	The study describes the significance of proposed model and provides insights about the application of the model in prediction and management of novel cybersecurity challenges.
IC3	Research objectives are clearly defined in the study.
IC4	The study proposes a new model or provides details of employing existing economics models in cybersecurity domain.
IC5	The study focuses on cybersecurity domain (i.e., not only information security, cyber-physical systems security, etc.).

Table 7. Quality assessment criteria (QAC).

ID	Description
QAC1	Are the research objectives clearly defined in the study?
QAC2	Does the study propose an artifact, or provide an analysis or extension of an existing artifact?
QAC3	Is the artifact clearly defined and validated in the study?
QAC4	Is the artifact compared to existing artifacts?
QAC5	Does the study provide insights and implications about the role and importance of the proposed artifact?
QAC6	Does the study consider the novel and emerging problems within the context of cybersecurity?

6. Data Synthesis

In this section, we investigate the selected studies listed in Table 8 to answer the research questions in Table 2.

Table 8. The list of the selected studies.

ID	Title	Year
[S01]	Institutional influences on information systems security innovations [125]	2012
[S02]	Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints [18]	2013
[S03]	A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis [126]	2014
[S04]	The impact of information sharing on cybersecurity underinvestment: A real options perspective [127]	2015
[S05]	Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment [128]	2019
[S06]	Cybersecurity investments in a two-echelon supply chain with third-party risk propagation [20]	2020
[S07]	Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers [120]	2016
[S08]	Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth [25]	2020
[S09]	Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements [129]	2013
[S10]	Coordination in network security games: A monotone comparative statics approach [83]	2012
[S11]	A game theory model of cybersecurity investments with information asymmetry [86]	2015
[S12]	Competitive cyber-insurance and internet security [130]	2010
[S14]	Increasing cybersecurity investments in private sector firms [131]	2015
[S15]	Should your firm invest in cyber risk insurance? [132]	2015
[S16]	Returns to information security investment: Endogenizing the expected loss [133]	2014
[S17]	Security investment and information sharing under an alternative security breach probability function [134]	2014
[S18]	The economic cost of publicly announced information security breaches: empirical evidence from the stock market [135]	2003
[S19]	Secure or Insure? A Game-Theoretic Analysis of Information Security Games [136]	2008
[S13]	Allocation of resources to cybersecurity: The effect of misalignment of interest between managers and investors [137]	2015
[S20]	Measuring the cost of cybercrime [138]	2013
[S21]	Investment decision on information system security: A scenario approach [98]	2009
[S22]	The economics of cybersecurity: Principles and policy options [113]	2010
[S23]	Security decision support challenges in data collection and use [139]	2010
[S24]	Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment [140]	2013
[S25]	The economics of information security investment [27]	2002
[S26]	Sharing information on computer systems security: An economic analysis [141]	2003
[S27]	Robustness of optimal investment decisions in mixed insurance/investment cyber risk management [100]	2020
[S28]	Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem [142]	2021

RQ1. What are the characteristics of an efficient cybersecurity economic model?

Economic models are theoretical constructs and conceptual frameworks that aid in the understanding, illustrating, and/or prediction of human behavior and complex processes. These models are methodologically used to investigate, theorize, and establish argumentative frameworks that represent the real world. The literature of cybersecurity economics shows that this area is being treated as an interdisciplinary field. Accordingly, the models proposed in this field draw concepts and techniques from a number of different disciplines, including organizational studies, complexity science, psychology, computer science, and sociology. Although each of the disciplines describes an efficient model in its own distinct way, nevertheless, when examined together, the scholars express efficient cybersecurity economic models as having five main properties. These properties go beyond the classical assumptions of rationality, optimization, and dynamic consistency. We believe that such assumptions are better considered as hypotheses that should be tested or conjectures that should be proved, and not fundamental characteristics of efficient economic models.

- Simplicity: The principle of simplicity has been largely accepted in science and it has been applied in different fields including economics. In the scientific methods, simple or parsimonious models prevent the researchers from manipulating the model so that it overfits the available facts by relying on relatively few special assumptions. Overfitting is a modeling error that occurs when a model works well in a given situation but fails to make accurate and reliable out-of-sample predictions. For example, [S01] incorporates a large set of qualitative biases. This model is non-parsimonious since the selective combination of those biases enables the researcher to adjust the model so that it can explain almost any pattern of observations. Likewise, complex budget constraints in [S02], makes the model relatively non-parsimonious. It can be argued that more flexible models enable the researchers to combine many elements and factors in the real world. However, this produces a false impression that the model has real explanatory power whereas it just makes it easy to explain in-sample data.
- Generalizability: If the results of a model are broadly applicable to a wide range of settings, the model is said to have good generalizability. The generalizability of a model's results depends on the researcher's ability to separate the "relevant" from the "irrelevant" facts of the study, and then carry forward a judgment about the relevant facts [143]. This would be easy if we always knew what might eventually turn out to be relevant. For example, uncertainty and complexity of the problems in [S02] and [S03] have caused to propose models with poor generalizability. As we mentioned earlier, agents make intertemporal choices within the context of cybersecurity economics. Therefore, a generalizable model of intertemporal choice (e.g., [S10]) could be used to study decisions with consequences that occur in the near-term and long-term future. Studies such as [S19], [S20], and [S21] attempted to propose generalizable models to unveil important patterns in systems' behavior.
- Empirical verifiability, applicability, and reproducibility: The empirically verifiable models are consistent with the available data and do not generate predictions that can be falsified by the data. If the researcher figures out that his model is empirically verifiable only if a certain effect is not present, then he must specify the domain of applicability of his model. The models are not intended to have universal applicability. They can be specialized to cases in which the arguments are evaluated. For example, models with homogeneous agents (e.g., [S12]) do not provide an ideal test for real-word settings that agents are characterized by their own culture, structure, machines, and methods. However, as argued in [S23] and [S24], the researchers have restricted their model to situations in which this effect is absent by stating the domain assumptions.
- Predictive precision: High predictive precision is desirable to facilitate model evaluation. This characteristic refers to how close the model's predictions are to the observed values. For example, [S07] allows a prospective test of theoretical understanding to generate testable predictions in changes that could occur in regulatory systems, depending on the combination of operators' incentives. Models with predictive precision are useful tools for decision makers who are trying to forecast future events or the consequences of new policies [144].

- Tractability: The degree to which a model admits convenient analysis and demands time, or other computational resources, with increasing its input size, is captured by tractability of a model. For example, [S11] is easy to implement and is manageable for more complex problems. However, [S14] and [S09] have not been able to provide a feasible solution. Consequently, they ignored the interaction among the agents in their proposed models to avoid an intractable problem.

RQ2. What challenges have been addressed by proposing the existing economic models?

Based on the selected studies, we identified issues and challenges that have been addressed and discussed by the literature of cybersecurity economics. We have classified these challenges into five categories. We acknowledge that this list is not exhaustive. However, it covers the most important problems that have been tackled or are yet to be studied in depth (e.g., rent-seeking behavior and lock-in). We discussed several of these challenges, such as investment and policies, as the main core issues of cybersecurity economics, in Section 4. Here, we outline the rest of issues that have received wide attention as well.

- **Budgeting** is an integral part of running any business efficiently and effectively. A budget is an estimation of revenue and expenses over a specified future period of time, and it can be made for a person, a group of people, a business, or a government. The budget development process plays a vital role in setting goals, measuring outcomes, and planning for contingencies.
  - *Investment* is a part of an overall budget development and expenditure management processes. Finding optimal investment strategies to balance cybersecurity risks and spending in security measures and controls has been a topic of major importance in cybersecurity economics.
  - *Externalities* or spillover effects occur when the benefits or costs of providing cybersecurity are not fully reflected in the budget development process. Overcoming externalities, both from public and private sectors, is important to avoid future budget deficiencies. Regulation is considered the most common solution to offset the effects of externalities [114].
  - Insurance is a contract in which an agent receives financial protection against losses from an insurance company. Insurance policies are used to hedge against the cybersecurity risks and cover the business' liabilities in the event of a cyber attack. By increasing the severity of financial consequences of cyber attacks, more businesses are turning to cybersecurity insurances. The literature of cybersecurity insurance has been focusing on determining how much cyber insurance businesses need to help insurers to understand the demand [145]. Moreover, uncertainty of outcomes, reinsurance (i.e., insurers lay off the risk to another capital source), and scale are problems that would suggest an increase in prices, hardening risk transfer, and influx of capital [S27].
- **Economic efficiency**, depending on the context, has various definitions in economics. For the sake of this review, we define economic efficiency as a situation in which no agent can make more profit without making at least one agent loss thereof.
  - *Misallocation of resources* indicates a state in which all resources are not allocated to serve each agent in the best way possible. The models that address this challenge are built based on the scarcity hypothesis. This hypothesis is the original source of methods such as the zero-sum games, comparative advantages, marginal returns, and time discount.
  - *The type of goods* that cybersecurity would treat would significantly influence the overall structures and success of cybersecurity economic models. According to Samuelson, there are four types of economics goods: private, common, club, and public goods [146]. The controversial arguments on how cybersecurity should be treated based on Samuelson's typology started in the last two decades [147].

Any of these types raise issues that might result in reduced economic efficiency through misallocation of resources, inefficient cybersecurity provision, and potential national and international insecurity. For example, attempts at managing free-riding problem ([S19]) and rent-seeking behavior is at the center of models that consider cybersecurity as a public good [148].

- **Interdependent risks** are common in today's hyper-connected world. The risks faced by any one agent depend not only on its choices but also on those of all others with which it is directly or indirectly interacting.
  - *Network effects* are phenomena whereby increased numbers of people or participants improve the value of a good or service. Positive and negative network effects have been extensively studied within the context of software security economics [149].
  - *Lock-in effects* refer to situations in which users are dependent on a single vendor or supplier for a specific service or product and cannot move to another vendor without substantial costs. Recently, companies (e.g., Apple and Microsoft) increase their lock-in through security mechanisms. This phenomenon can be investigated in terms of control, governance, and dominance of organizations or groups such as Trusted Computing Group within the security value chain.
  - *Supply chains risks* associated with digital transformation of supply chains globally are increasingly becoming part of the enterprise risk listing and supply chain management. Modeling the target system, identifying threats, and analyzing countermeasures are three main issues that require systematic studies and socio-technical analyses to mitigate this type of risk [150].
- **Information asymmetry** deals with the situation where one party possesses more information than the other party. A lack of equal information results in adverse selection and moral hazards. All of these economic weaknesses have the potential to lead to market failure. Moral hazard is a situation where there is a tendency to take undue risks because the costs are not borne by the party taking the risk. Our tendency toward technological ubiquity, the unclear relationships between technology manufacturer and user, the inherent complexity of technology, and the network effects inherent to connected technologies are some of the factors that help this failure [151].
- **Governance** effectively coordinates the security activities of organizations and enables the flow of security information and decisions around them. Governance defines the rules and procedures for decision making. Governance is important because it specifies the structure and distribution of rights and responsibilities among the different agents in the system.
  - *Coordination* among different agencies and stakeholders involved in performing cybersecurity functions and practices, such as response to threats or incidents and cyber crisis management, has been studied in terms of incentives, costs, and business alignment. However, there are still problems with regard to economic complexity of the coordination procedures and dependable enforcement of effective measures.
  - *Cybersecurity Policies, Regulations, and Rules (PRR)* are the areas that have involved public and private sectors in many forms of self- and co-regulations since the emergence of the internet. In this regard, the dominated notion is that cybersecurity policymaking and regulations require multifaceted strategies and recognition of the significant role that economic analysis plays to determine the actual need or effectiveness of these regulations [152].
- **Cybercrimes** are global and have strong externalities. Many academic studies and industrial documents examine the costs and losses caused by cybercrime. Some works estimate the overall costs, others evaluate the costs of individual countries, while industrial documents even measure losses of certain organizations regardless of or considering their size and technological development. For example, [S20] is one of the

first studies of measuring the costs of cybercrime. The authors continued this work seven years later to report major changes that significantly influenced the results of the original study [153].

- **Sustainability** of cybersecurity providers and services is increased by better formulation of business strategies and policies. For example, [S28] discusses how, to achieve sustainability of the digital ecosystems, finding a balance between the values obtained by the stakeholders is essential. If any of the stakeholders do not gain sufficient value, the entire ecosystem will collapse. Hence, promoting secure and sustainable properties is becoming a requirement in both development processes of cybersecurity products and services [154].

Table 9 shows the main challenges that are addressed by the selected studies. The diversity of these challenges shows that cybersecurity economics is not limited to the financial and budgeting issues, but it also covers politics, coordination, and other organizational topics.

Table 9. The main challenges addressed by the selected studies.

ID	Challenges
[S01]	Economic Efficiency and Governance
[S02]	Investment
[S03]	Supply Chain
[S04]	Investment and Information Sharing
[S05]	Investment
[S06]	Supply Chain and Investment
[S07]	Policies, Regulations, and Rules (PRR)
[S08]	Externalities
[S09]	Insurance
[S10]	Coordination and Network Effect
[S11]	Information Asymmetry
[S12]	Moral Hazard
[S13]	Misallocation of Resources
[S14]	Types of Goods and PRR
[S15]	Insurance
[S16]	Investment
[S17]	Investment and Information Sharing
[S18]	Economic Efficiencies
[S19]	Types of Goods
[S20]	Cybercrime
[S21]	Investment
[S22]	Policies, Regulations, and Rules (PRR)
[S23]	Governance
[S24]	Policies, Regulations, and Rules (PRR)
[S25]	Investment
[S26]	Information Sharing
[S27]	Insurance
[S28]	Sustainability

RQ3. What are the main issues faced by the current cybersecurity economic models?

Recently developed cybersecurity strategies and policies have recognized that cybersecurity is a continuously evolving phenomenon in a complex socio-technical system in which multistakeholder governance processes and multilateral approaches are required to enhance cybersecurity posture in organizations and nations. Despite this understanding, the field of cybersecurity economics continues to face challenges that limits the applicability, effectiveness, and functionality of proposed models and analysis. Here, we highlight five major challenges that have been pointed out in the literature of cybersecurity economics. The first challenge that has been extensively recognized in the literature is complexity. If organizations, societies, and markets are viewed as complex and out-of-equilibrium systems, understanding non-linear, adaptive, and evolutionary patterns which emerge from system dynamics and agents' behavior in network structures is important for researchers. To tackle this challenge, the researchers need to reconsider the dominant equilibrium thinking in their models and shift from focusing on proposing models to optimize and predict system equilibrium to manage the complexity of cybersecurity better. This has also been recognized in other areas such as financial market regulations [155], energy [156], and healthcare policies [157].

The second challenge is that most economic models rest on a number of assumptions that are not entirely realistic. For example, it is often assumed that the decision makers are assumed to be rational and to have perfect information. There is growing literature in economics that shows humans do not have the processing capacity to be perfectly rational, even if they had perfect and complete information. Therefore, any analysis of the results and application of the proposed models must consider the inaccuracies that compromises the model based on these assumption. In addition to the unrealistic assumptions, the model overlooks issues that are important to the question being studied, such as externalities and interdependencies. These concepts intertwine with bounded rationality, cognitive dispositions, and social preferences [37].

The third challenge is the difficulty in measurement and quantification of the psychometric variables, such as the perceived value of cybersecurity, perceived cyber risks, and willingness to pay/collaborate. When the researchers neglect these variables, their model cannot provide full explanations or correct predictions of the phenomenon under study. The lack of reliable instruments to determine the indicators of these latent constructs contribute to the difficulty in measuring them. Another important challenge is the tension between rigor and relevance across cybersecurity economics models. The models that are purely theoretical or expressed mathematically are prone to poor relevance and applicability. The main question here is if a tradeoff must exist between rigor and relevance. If yes, what is the right balance between rigor and relevance in the study? To answer these questions, the researchers need to understand the system, identify the significant constructs, and use scientific methods that promote the systematic uptake of research findings and other evidence-based practices into routine practice.

Finally, the fifth challenge is the arising problem of parameter identification in construction of models using econometrics. Econometrics is the application of statistical and mathematical methods using observational and empirical data to develop new theories or test hypotheses. In all of the preceding sections, we discussed that the behavior, structure and characteristics of the environment, and the agents that operate within it do have an influence on the cybersecurity posture of the system as a whole. However, the situation is complicated when it comes to empirically testing such propositions. As Manski has pointed out, the propensity of agent behavior can vary with the behavior of group (i.e., contagious effects) or with exogenous characteristics of the group (i.e., contextual effects). It also can be similar to the group as they face a similar institutional environment (i.e., correlated effects).

To give an example, suppose that we observe an increase in the cybersecurity spending of three aluminum companies (Norsk Hydro in Norway, Kaiser Aluminum in America, and Hindalco in India) in 2020. A natural inference would be that they raised their investment due to the perceived cyber risk after the cyber attack against Norsk Hydro in 2019. However, on careful investigation, we find Kaiser Aluminum raised its investment due to the adoption of new information technology systems [158] and Hindalco due to the huge investment in capacity building after unveiling major capacity expansion plans in UltraTech (another subsidiary of the Aditya Birla Group). The question then is how these two possibilities can be distinguished. If you want to determine the importance of network effect in this example, what is most lacking is dependable empirical evidence and observational data.

RQ4. What data is needed to reliably assess the performance of a cybersecurity economic model?

Adequate data are critical in verification, validation, and assessment of the proposed economic models. The models often assist the researchers in considering what kind of data is useful to provide a foundation for investigations and explorations. As we discussed in the RQ2, cybersecurity economic models are developed with respect to a particular phenomenon or class of phenomena (e.g., budgeting, regulations, economic efficiency, etc.). To explain the phenomenon and test the models' key implications, the researchers use different types of data. The selection of type might be justifiable with regard to the research questions, scientific method, and availability. In this review, we identify five data types that were used in the studies:

- Observational data are captured through observation of agent's and system's behavior and their interactions in the real world. It is collected using methods such as observation by human or artificial sensors and open-end surveys. Since observational data are captured in real-time, the reproducibility of data would be difficult or, in some cases, impossible. [S03] has used observational data to assess the performance of the proposed model.
- Empirical data are also collected by means of senses and observation of behavior and patterns. However, this process is through experiments. Within the experiments, the experimenter can either control the conditions or not. Whereas the collected data from controlled and uncontrolled experiments can be qualitatively similar, their quantitative differences could be significant. Empirical data are captured when the conditions are not controlled, and they will be recorded along with the results. This type of data is often reproducible. Studies [S01], [S05], [S08], and [S14] have used empirical data to validate and assess the performance of their proposed models.
- Simulation data are generated by imitating the operation of agents in a real-world process or systems over time using computer-aided modeling and simulations. This type of data is suitable for theoretical verification and testing any combination of parameters in the model. Studies [S02], [S06], and [S28] use simulation data for the purpose of their research.
- Derived data use existing data, often from different data sets, to generate new data through transformation by arithmetic/mathematical formula and aggregation. Compiled databases or data derived from the game theoretical analyses are good examples of this data type. Studies [S09], [S10], [S11], [S12], and [S13] have used derived data to assess the performance of their proposed models.
- Projected data are useful in the context of policy evaluations when data do not exist or are scarce. These data can also be used to validate the results obtained from simulation of models. [S04] and [S07] are the two studies that have used projected data to show the insights of their proposed models.

However, there are several challenges along the way. Data are expensive to collect, difficult to harmonize, and, sometimes, difficult to realize if they are relevant to a specific model [159]. Furthermore, considering the fact that digital technologies and business processes are fast changing, data tend to become outdated and must be refreshed and improved. This delineates a necessary revision of the way we collect, use, communicate, and share data. Various biases such as selection bias [e.g., S01], publication bias, reporting bias, confirmation bias [e.g., S08], and funding bias might also be introduced in these processes. Therefore, data plays an increasingly significant role in answering the crucial question of the determinants of success or failure of economics models. UK Data Archive suggests a guide [160] to managing and sharing research data that can be useful in fields such as cybersecurity economics.

RQ5. How has cybersecurity economics contributed to providing solutions for known and unknown problems within the cybersecurity domain?

Our literature review shows that cybersecurity economics has had both descriptive and prescriptive roles. In its descriptive role, cybersecurity economics not only explains how various economic forces affect the cybersecurity posture of an organization or state but also predicts the consequences of the decisions made by it. In its prescriptive role, however, cybersecurity economics prescribes the rules, regulations, and policies for the improvement of decision making by organizations or governments so that they can achieve their objectives efficiently. However, as Colander states [29], to know whether you can apply economic theories to real-world settings, you must know about economic institutions, and cybersecurity is not an exception. Organizations, governments, and cultural norms are all examples of institutions that have social, political, and regulatory dimensions which all can impact on the sustainability of cybersecurity in those institutions. Therefore, it is important to understand the institutions to gain insight on how economic theories function. It also helps both researchers and practitioners who employ the proposed models account for the differences between the ways that models work in reality and throughout their experiments.

Since the inception of the field in 2000, the general acceptance of cybersecurity economics as a competent approach to tackle the challenges that were highlighted in RQ2 is increasing. A wide range of socio-technical artifacts such as decision support systems, modeling and simulation tools, governance strategies, evaluation methods, and change interventions have been constructed in this field of research. Understanding and positioning the knowledge contribution of the research projects in this field is necessary to employ their findings in the day-to-day routines and the longer-term direction of the agents. As Marc and Smith stated, "real problems must be properly conceptualized and represented, and appropriate techniques for their solution must be constructed" [161]. Our review reveals that this has been achieved by combining practical knowledge and scientific rigor. On the whole, to answer this question, we used the Design Science Research Knowledge Contribution Framework to classify the theoretical and empirical contributions of the selected studies based on their research problems and proposed solutions.

As depicted in Figure 3, most of the proposed solutions in the selected studies result in improvement or exaptation of the artifacts. These types of research is also common in information system studies, where new problems emerge with the changes in digital ecosystem. The key challenges in these two quadrant is to clearly demonstrate the improvement and exaptation properly advance the existing knowledge.

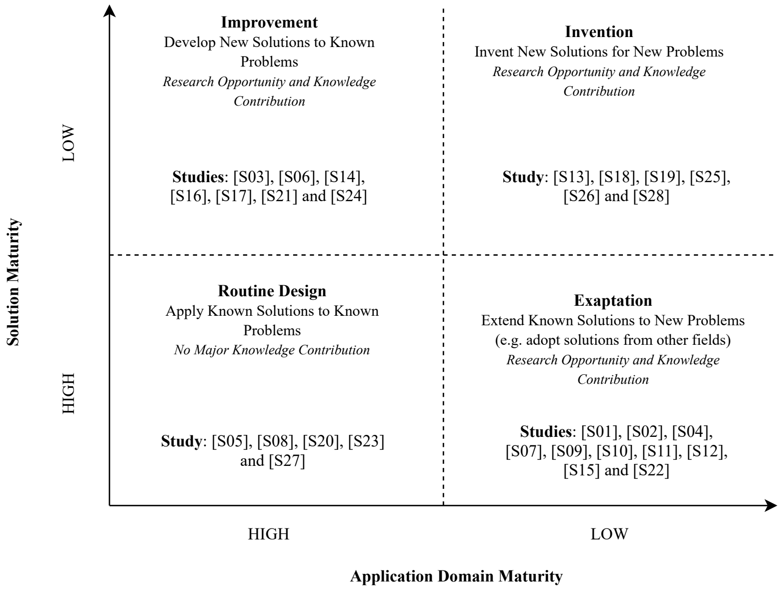
Improvement
Develop New Solutions to Known Problems
Research Opportunity and Knowledge Contribution
Studies: [S03], [S06], [S14], [S16], [S17], [S21] and [S24]
Invention
Invent New Solutions for New Problems
Research Opportunity and Knowledge Contribution
Study: [S13], [S18], [S19], [S25], [S26] and [S28]
Routine Design
Apply Known Solutions to Known Problems
No Major Knowledge Contribution
Study: [S05], [S08], [S20], [S23] and [S27]
Exaptation
Extend Known Solutions to New Problems (e.g. adopt solutions from other fields)
Research Opportunity and Knowledge Contribution
Studies: [S01], [S02], [S04], [S07], [S09], [S10], [S11], [S12], [S15] and [S22]
LOW
HIGH
Solution Maturity
HIGH
LOW
Application Domain Maturity

Figure 3. Classification of selected studies based on DSR Knowledge Contribution Framework.

7. Conclusions

Interweaving dimensions of theory and practice, this paper reflected on some of the issues in the research on cybersecurity economics, emphasizing, in particular, the constructive and complexity aspects of the field. Moreover, the paper analyzes different cybersecurity economics models described in the scientific literature and identifies the relevant properties to cybersecurity economics. To this end, we conducted a transdisciplinary meta-narrative literature review in which we identified 628 articles on cybersecurity economics models. Out of these articles, we selected 28 studies based on an exhaustive selection process. The findings of the review and our observations suggest remarkable, persistent effects of factors that contribute to sustainable cybersecurity posture in reality. Drawing on the contributions of many studies, most of which are cited in this survey, this study provided an overview of the theoretical and empirical sides of the growing literature on cybersecurity economics.

The literature of cybersecurity economics has covered a broad range of topics from budgeting to policies and regulation. Both quantitative and qualitative tools have been used to provide important insights from various research fields and disciplines into this field. However, complexity science, interdisciplinary knowledge, ethical and moral aspects, and the importance of institutions and social rules could be included more explicitly. Furthermore, more than half of the reviewed studies have extended the known solutions to new problems (i.e., exaptation). This shows that the maturity of the cybersecurity economics field is growing and provides the researchers with more research opportunities. Furthermore, the empirical evidence shows that the practical implications of the research in this field can be successfully implemented for sustainable solutions if the researchers eliminate the most pressing anomalies and enhance the maturity of the application domain and developed solutions. Our paper, "Multi-paradigmatic Approaches in Cybersecurity Economics" [162], suggests five core themes to reflect on the further development on paradigm, methodologies, and hypotheses in which the research on cybersecurity economics has been based on. These themes are interrelated and shape a multi-paradigmatic structure of the field. They can also be known as the characteristics of a new approach in cybersecurity economics. We recommend that researchers strengthen their capabilities of integration of these characteristics and comparability across models. The latter is important to identify the strengths and weaknesses of different models and synergies in model advancement by exploiting the model structure of the different disciplines' knowledge base.

We also argue that the goal of cybersecurity economics is, in addition to the suggested financial and budgeting tools, to explain and predict the behavior and patterns of the agents and systems, design institutions, and recommend sustainable policies and regulations. In the context of cybersecurity, the policymakers are, increasingly, in urgent need of new short- and long-term planning tools capturing the relevant features of the modern digital ecosystem, including complexity, uncertainty, bounded rationality, and out-of-equilibrium. We need further research on exploring new, meaningful, and clear ways to interpret, compare, and communicate the results and policy insights of the proposed models so that policymakers and decision makers fully understand the relevance of these findings.

Finally, our review does not investigate some important questions such as: Can different macro- and microeconomics models be connected to each other and, if so, what are the benefits of doing so? How could synergies in model building be better exploited? What are the best approaches to combine and compare the different models to gain a more comprehensive picture of the practical implications? How and to what extent are these implications determined by the model structure? These questions warrant further research and analysis on the topic. Another limitation of this study is excluding grey literature from the selected studies. While we acknowledge that business reports and analyses (e.g., publications by Deloitte, PWC, EY, and KPMG) contribute to the maturity of the cybersecurity economics research significantly, this study covered academic journals and conference papers. Hence, selecting all the relevant publications is not guaranteed.

Future studies can expand the study domain to include editorial papers, white papers, and industrial reports and insights.

Author Contributions: Conceptualization, M.K., S.J.K. and H.Ø.; methodology, M.K., S.J.K. and H.Ø.; validation, M.K., S.J.K. and H.Ø.; formal analysis, M.K; investigation, M.K. and S.J.K.; resources, M.K. and S.J.K.; data curation, M.K.; writing—original draft preparation, M.K.; writing—review and editing, M.K. and H.Ø.; visualization, M.K.; supervision, S.J.K. and H.Ø.; project administration, M.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: Data supporting the results are found within the body of the paperand in referenced works.

Acknowledgments: The authors greatly appreciate the thoughtful comments and suggestions of the anonymous reviewers.

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

References

1. Courtney, R.H., Jr. A systematic approach to data security. *Comput. Secur.* **1982**, *1*, 99–112. [CrossRef]
2. Dixon, P.B.; Jorgenson, D. *Handbook of Computable General Equilibrium Modeling*; Elsevier: Newnes, UK, 2012; Volume 1.
3. McLennan, M. *The Global Risks Report*, 16th ed.; The World Economic Forum: Geneva, Switzerland, 2021.
4. Lewis, J.; Smith, Z.; Lostri, E. The Hidden Costs of Cybercrime (CSIS, 2020). 2021. Available online: https://www.csis.org/analysis/hidden-costs-cybercrime (accessed on 17 August 2021).
5. Verizon. *Data Breach Investigations Report 2020*; Technical Report; Verizon: New York, NY, USA, 2020. [CrossRef]
6. Cat, J. The Unity of Science. In *The Stanford Encyclopedia of Philosophy*; Zalta, E.N., Ed.; Metaphysics Research Lab, Stanford University: Stanford, CA, USA, 2017.
7. Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [CrossRef]
8. Brookson, C.; Cadzow, S.; Eckmaier, R.; Eschweiler, J.; Gerber, B.; Guarino, A.; Rannenberg, K.; Shamah, J.; Gorniak, S. *Definition of Cybersecurity-Gaps and Overlaps in Standardisation*; ENISA: Heraklion, Greece, 2015.
9. ISO/IEC27002. *Information Technology–Security Techniques–Code of Practice for Information Security Controls, (AS ISO/IEC 27002: 2015)*; International Organization for Standardization: Geneva, Switzerland, 2015.
10. Coulon, Y. *Rational Investing with Ratios: Implementing Ratios with Enterprise Value and Behavioral Finance*; Springer Nature: Cham, Switzerland, 2019.
11. Straub, D.; Rai, A.; Klein, R. Measuring firm performance at the network level: A nomology of the business impact of digital supply networks. *J. Manag. Inf. Syst.* **2004**, *21*, 83–114. [CrossRef]
12. Moody, D.L.; Walsh, P. Measuring the Value of Information—An Asset Valuation Approach. In Proceedings of the Seventh European Conference on Information Systems (ECIS'99), Copenhagen Business School, Frederiksberg, Denmark, 23–25 June 1999; pp. 496–512.
13. Henderson, S.; Peirson, G.; Herbohn, K.; Howieson, B. *Issues in Financial Accounting*; Pearson Higher Education: Melbourne, Australia, 2015.
14. Godfrey, J.; Hodgson, A.; Tarca, A.; Hamilton, J.; Holmes, S. *Accounting Theory*; Wiley and Sons: Hoboken, NJ, USA, 2010.
15. Arora, A.; Hall, D.; Piato, C.; Ramsey, D.; Telang, R. Measuring the risk-based value of IT security solutions. *IT Prof.* **2004**, *6*, 35–42. [CrossRef]
16. Bistarelli, S.; Dall'Aglio, M.; Peretti, P. Strategic games on defense trees. In *International Workshop on Formal Aspects in Security and Trust*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 1–15.
17. Shirtz, D.; Elovici, Y. Optimizing investment decisions in selecting information security remedies. *Inf. Manag. Comput. Secur.* **2011**, *19*, 95–112. [CrossRef]
18. Huang, C.D.; Behara, R.S. Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *Int. J. Prod. Econ.* **2013**, *141*, 255–268. [CrossRef]
19. Ezhei, M.; Ladani, B.T. Interdependency analysis in security investment against strategic attacks. In *Information Systems Frontiers*; Springer: New York, NY, USA, 2018; pp. 1–15.
20. Li, Y.; Xu, L. Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. *Int. J. Prod. Res.* **2020**, *59*, 1216–1238. [CrossRef]
21. Schatz, D.; Bashroush, R. Economic valuation for information security investment: A systematic literature review. *Inf. Syst. Front.* **2017**, *19*, 1205–1228. [CrossRef]

22. Ekelund, S.; Iskoujina, Z. Cybersecurity economics–balancing operational security spending. *Inf. Technol. People* **2019**, *32*, 1318–1342. [CrossRef]
23. Anderson, R.; Schneier, B. Guest Editors' Introduction: Economics of Information Security. *IEEE Secur. Priv.* **2005**, *3*, 12–13. [CrossRef]
24. Neubauer, T.; Klemen, M.; Biffl, S. Secure business process management: A roadmap. In Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, 20–22 April 2006; p. 8.
25. Ahmed, E.M. Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth. *J. Knowl. Econ.* **2020**, *2020*, 1–19. [CrossRef]
26. Rathod, P.; Hämäläinen, T. A novel model for cybersecurity economics and analysis. In Proceedings of the 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland, 21–23 August 2017; pp. 274–279.
27. Gordon, L.A.; Loeb, M.P. The economics of information security investment. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2002**, *5*, 438–457. [CrossRef]
28. Bojanc, R.; Jerman-Blažič, B. A quantitative model for information-security risk management. *Eng. Manag. J.* **2013**, *25*, 25–37. [CrossRef]
29. David, C.C. *Microeconomics*; McGraw-Hill Education: New York, NY, USA, 2020.
30. Crumpler, W.; Lewis, J.A. *Cybersecurity Workforce Gap*; Center for Strategic and International Studies (CSIS): Washington, DC, USA, 2019.
31. DellaVigna, S. Psychology and economics: Evidence from the field. *J. Econ. Lit.* **2009**, *47*, 315–372. [CrossRef]
32. Broadbent, D.E. *Perception and Communication*; Elsevier: Amsterdam, The Netherlands, 2013.
33. Stirling, A. Risk, uncertainty and precaution: Some instrumental implications from the social sciences. In *Negotiating Environmental Change: New Perspectives from the Social Sciences*; Edward Elgar: Cheltenham, UK, 2003; pp. 33–76.
34. Cavusoglu, H.; Mishra, B.; Raghunathan, S. A model for evaluating IT security investments. *Commun. ACM* **2004**, *47*, 87–92. [CrossRef]
35. Huang, C.D.; Hu, Q.; Behara, R.S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *Int. J. Prod. Econ.* **2008**, *114*, 793–804. [CrossRef]
36. Hoo, K.J.S. How Much Is Enough? A Risk Management Approach to Computer Security. Ph.D. Thesis, Stanford University, Stanford, CA, USA, 2000.
37. Kianpour, M.; Øverby, H.; Kowalski, S.J.; Frantz, C. Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties. In *International Conference on Human-Computer Interaction*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 149–163.
38. Bryan, J. *A Better Way to Manage Third-Party Risk*; Gartner: Stanford, CA, USA, 2019.
39. Colander, D.; Holt, R.; Rosser, B., Jr. The changing face of mainstream economics. *Rev. Political Econ.* **2004**, *16*, 485–499. [CrossRef]
40. Cavusoglu, H.; Raghunathan, S.; Yue, W.T. Decision-theoretic and game-theoretic approaches to IT security investment. *J. Manag. Inf. Syst.* **2008**, *25*, 281–304. [CrossRef]
41. Cremonini, M.; Nizovtsev, D. Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies. In Proceedings of the 4th Workshop on the Economics of Information Security, Boston, MA, USA, 2–3 June 2005.
42. Schechter, S.E.; Smith, M.D. How much security is enough to stop a thief? In Proceedings of the International Conference on Financial Cryptography, Guadeloupe, France, 27–30 January 2003; pp. 122–137.
43. Leeson, P.T.; Coyne, C.J. The economics of computer hacking. *JL Econ. Policy* **2005**, *1*, 511.
44. Huang, C.D.; Behara, R.S.; Goo, J. Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decis. Support Syst.* **2014**, *61*, 1–11. [CrossRef]
45. Miura-Ko, R.A.; Yolken, B.; Mitchell, J.; Bambos, N. Security decision-making among interdependent organizations. In Proceedings of the 2008 21st IEEE Computer Security Foundations Symposium, Pittsburgh, PA, USA, 23–25 June 2008; pp. 66–80.
46. Kayworth, T.; Whitten, D. Effective information security requires a balance of social and technology factors. *MIS Q. Exec.* **2010**, *9*, 2012–2052.
47. Gordon, L.A.; Loeb, M.P. *Managing Cybersecurity Resources: A Cost-Benefit Analysis*; McGraw-Hill: New York, NY, USA, 2006; Volume 1.
48. Huang, C.D.; Behara, R.S.; Hu, Q. Economics of information security investment. In Proceedings of the 5th Workshop on the Economics of Information Security (WEIS), Cambridge, UK, 26–28 June 2006.
49. Kersting, F.; Obst, D. Behavioral Economics. Exploring Economics. Available online: https://www.exploring-economics.org/en/orientation/behavioral-economic (accessed on 12 June 2021).
50. Paul, J.A.; Wang, X.J. Socially optimal IT investment for cybersecurity. *Decis. Support Syst.* **2019**, *122*, 113069. [CrossRef]
51. Koepke, P. *Cybersecurity Information Sharing Incentives and Barriers*; Sloan School of Management at MIT University: Cambridge, MA, USA, 2017.
52. Xu, M.; Hua, L. Cybersecurity insurance: Modeling and pricing. *N. Am. Actuar. J.* **2019**, *23*, 220–249. [CrossRef]
53. Wang, S.S. Integrated framework for information security investment and cyber insurance. *Pac.-Basin Financ. J.* **2019**, *57*, 101173. [CrossRef]
54. Tosh, D.K.; Shetty, S.; Sengupta, S.; Kesan, J.P.; Kamhoua, C.A. Risk management using cyber-threat information sharing and cyber-insurance. In *International Conference on Game Theory for Networks*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 154–164.

55. Rowe, B.; Pokryshevskiy, I.D.; Link, A.N.; Reeves, D.S. Economic analysis of an inadequate cyber security technical infrastructure. In *National Institute of Standards and Technology Planning Report*; NIST: Gaithersburg, MD, USA 2013.
56. Blythe, J.M.; Johnson, S.D.; Manning, M. What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Sci.* **2020**, *9*, 1. [CrossRef]
57. Grossklags, J.; Acquisti, A. *When 25 Cents is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information*; In Proceedings of the 6th Workshop on the Economics of Information Security (WEIS), Pittsburgh, PA, USA, 7–8 June 2007.
58. Renaud, K.; Otondo, R.; Warkentin, M. "This is the way 'I'create my passwords"... does the endowment effect deter people from changing the way they create their passwords? *Comput. Secur.* **2019**, *82*, 241–260. [CrossRef]
59. Fineberg, V. BECO: Behavioral Economics of Cyberspace Operations. *Games People Play. Behav. Secur.* **2014**, *2*, 20.
60. Keysight Surveys. *Security Operations Effectiveness*; Keysight Technologies: Santa Rosa, CA, USA, 2020.
61. Dong, K.; Lin, R.; Yin, X.; Xie, Z. How does overconfidence affect information security investment and information security performance? *Enterp. Inf. Syst.* **2019**, *15*, 1–18. [CrossRef]
62. de Bruijn, H. *The Art of Framing: How Politicians Convince Us That They Are Right*; Amsterdam University Press: Amsterdam, The Netherlands, 2017.
63. Sivan-Sevilla, I. Framing and governing cyber risks: Comparative analysis of US Federal policies [1996–2018]. *J. Risk Res.* **2019**, *24*, 692–720. [CrossRef]
64. Lawson, S. Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *J. Inf. Technol. Politics* **2013**, *10*, 86–103. [CrossRef]
65. Wheeler, E. Framing cyber security as a business risk. *Cyber Secur. Peer-Rev. J.* **2018**, *2*, 202–210.
66. Ween, A.; Dortmans, P.; Thakur, N.; Rowe, C. Framing cyber warfare: An analyst's perspective. *J. Def. Model. Simul.* **2019**, *16*, 335–345. [CrossRef]
67. Dortmans, P.J.; Thakur, N.; Ween, A. Conjectures for framing cyberwarfare. *Def. Secur. Anal.* **2015**, *31*, 172–184. [CrossRef]
68. Tversky, A.; Kahneman, D. The framing of decisions and the psychology of choice. *Science* **1981**, *211*, 453–458. [CrossRef]
69. de Bruijn, H.; Janssen, M. Building cybersecurity awareness: The need for evidence-based framing strategies. *Gov. Inf. Q.* **2017**, *34*, 1–7. [CrossRef]
70. Mak, J.K.L.; Cho, H. Framing Smart Nation: A moderated mediation analysis of frame-focus effects. *Inf. Commun. Soc.* **2019**, *35*, 1–21. [CrossRef]
71. Cheung-Blunden, V.; Cropper, K.; Panis, A.; Davis, K. Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences. *Emotion* **2019**, *19*, 1353. [CrossRef]
72. Renaud, K.; Dupuis, M. Cyber security fear appeals: Unexpectedly complicated. In Proceedings of the New Security Paradigms Workshop, Costa Rica, CA, USA, 23–26 September 2019; pp. 42–56.
73. Nelson, N.; Madnick, S. *Studying the Tension between Digital Innovation and Cybersecurity*; Sloan School of Management, MIT: Cambridge, MA, USA, 2017.
74. Bailetti, T.; Craigen, D. Examining the Relationship Between Cybersecurity and Scaling Value for New Companies. *Technol. Innov. Manag. Rev.* **2020**, *10*, 62–69. [CrossRef]
75. Garud, R.; Karnøe, P. Path creation as a process of mindful deviation. *Path Depend. Creat.* **2001**, *138*, 38.
76. Shiozawa, Y.; Morioka, M.; Taniguchi, K. Microfoundations of evolutionary economics. In *Microfoundations of Evolutionary Economics*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1–52.
77. Kuerbis, B.; Badiei, F. Mapping the cybersecurity institutional landscape. *Digit. Policy Regul. Gov.* **2017**, *19*, 33. [CrossRef]
78. Lindsay, J.R. Restrained by design: The political economy of cybersecurity. *Digit. Policy Regul. Gov.* **2017**, *19*, 493–514. [CrossRef]
79. Anderson, R. Why Information Security is Hard-An Economic Perspective. In Proceedings of the 17th Annual Computer Security Applications Conference, ACSAC '01, New Orleans, LA, USA, 10–14 December 2001; IEEE Computer Society: Washington, DC, USA, 2001; p. 358.
80. Brecht, M.; Nowey, T. A closer look at information security costs. In *The Economics of Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 3–24.
81. Baryshnikov, Y. IT Security Investment and Gordon-Loeb's 1/e Rule. In Proceedings of the 11th Workshop on the Economics of Information Security (WEIS), Berlin, Germany, 25–26 June 2012.
82. Willemson, J. On the Gordon & Loeb Model for Information Security Investment. In Proceedings of the 5th Workshop on the Economics of Information Security (WEIS), Cambridge, UK, 26–28 June 2006.
83. Lelarge, M. Coordination in network security games: A monotone comparative statics approach. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 2210–2219. [CrossRef]
84. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; Zhou, L. Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *J. Inf. Secur.* **2014**, *6*, 24. [CrossRef]
85. Patwary, A.A.N.; Naha, R.K.; Garg, S.; Battula, S.K.; Patwary, M.A.K.; Aghasian, E.; Amin, M.B.; Mahanti, A.; Gong, M. Towards Secure Fog Computing: A Survey on Trust Management, Privacy, Authentication, Threats and Access Control. *Electronics* **2021**, *10*, 1171. [CrossRef]
86. Nagurney, A.; Nagurney, L.S. A game theory model of cybersecurity investments with information asymmetry. *Netnomics Econ. Res. Electron. Netw.* **2015**, *16*, 127–148. [CrossRef]

87. Fielder, A.; Panaousis, E.; Malacaria, P.; Hankin, C.; Smeraldi, F. Decision support approaches for cyber security investment. *Decis. Support Syst.* **2016**, *86*, 13–23. [CrossRef]
88. Hota, A.R.; Sundaram, S. Interdependent security games on networks under behavioral probability weighting. *IEEE Trans. Control. Netw. Syst.* **2016**, *5*, 262–273. [CrossRef]
89. Abdallah, M.; Naghizadeh, P.; Hota, A.R.; Cason, T.; Bagchi, S.; Sundaram, S. The impacts of behavioral probability weighting on security investments in interdependent systems. In Proceedings of the 2019 American Control Conference (ACC), Philadelphia, PA, USA, 10–12 July 2019; pp. 5260–5265.
90. Abdallah, M.; Naghizadeh, P.; Hota, A.R.; Cason, T.; Bagchi, S.; Sundaram, S. Behavioral and Game-Theoretic Security Investments in Interdependent Systems Modeled by Attack Graphs. *IEEE Trans. Control Netw. Syst.* **2020**, *7*, 1585–1596. [CrossRef]
91. Sonnenreich, W.; Albanese, J.; Stout, B. Return on security investment (ROSI)—A practical quantitative model. *J. Res. Pract. Inf. Technol.* **2006**, *38*, 45.
92. Pontes, E.; Guelfi, A.E.; Silva, A.A.; Kofuji, S.T. A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI). In *Risk Management in Environment, Production and Economy*; InTech: Rijeka, Croatia, 2011; pp. 149–170.
93. Smith, M.D.; Paté-Cornell, M.E. Cyber risk analysis for a smart grid: How smart is smart enough? a multiarmed bandit approach to cyber security investment. *IEEE Trans. Eng. Manag.* **2018**, *65*, 434–447. [CrossRef]
94. Čapko, Z.; Aksentijević, S.; Tijan, E. Economic and financial analysis of investments in information security. In Proceedings of the 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 26–30 May 2014; pp. 1550–1556.
95. Sheen, J. Fuzzy economic decision-models for information security investment. In Proceedings of the 9th International Conference on Instrumentation, Measurement, Circuits and Systems, IMCAS'10, Hangzhou, China, 11–13 April 2010; pp. 141–147.
96. Jerman-Blažič, B. Quantitative model for economic analyses of information security investment in an enterprise information system. *Organizacija* **2012**, *45*, 276–288.
97. Jerman-Blažič, B. Towards a standard approach for quantifying an ICT security investment. *Comput. Stand. Interfaces* **2008**, *30*, 216–222.
98. Huang, C.D.; Goo, J. Investment decision on information system security: A scenario approach. In Proceedings of the 15th Americas Conference on Information Systems, San Francisco, CA, USA, 6–9 August 2009; p. 571.
99. Jerman-Blažič, B. An economic modelling approach to information security risk management. *Int. J. Inf. Manag.* **2008**, *28*, 413–422.
100. Mazzoccoli, A.; Naldi, M. Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. *Risk Anal.* **2020**, *40*, 550–564. [CrossRef] [PubMed]
101. Hagen, J.M.; Albrechtsen, E.; Hovden, J. Implementation and effectiveness of organizational information security measures. *Inf. Manag. Comput. Secur.* **2008**, *16*, 377–397. [CrossRef]
102. Mayadunne, S.; Park, S. An economic model to evaluate information security investment of risk-taking small and medium enterprises. *Int. J. Prod. Econ.* **2016**, *182*, 519–530. [CrossRef]
103. Miaoui, Y.; Boudriga, N. Enterprise security investment through time when facing different types of vulnerabilities. *Inf. Syst. Front.* **2019**, *21*, 261–300. [CrossRef]
104. Elsner, W.; Heinrich, T.; Schwardt, H. *The Microeconomics of Complex Economies*; Academic Press: Cambridge, MA, USA, 2014.
105. Corbet, S.; Gurdgiev, C. What the hack: Systematic risk contagion from cyber events. *Int. Rev. Financ. Anal.* **2019**, *65*, 101386. [CrossRef]
106. Szubartowicz, E.; Schryen, G. Timing in information security: An event study on the impact of information security investment announcements. *J. Inf. Syst. Secur.* **2020**, *16*, 3–31.
107. Tisdale, S.M. Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. *Issues Inf. Syst.* **2015**, *16*, 191–198.
108. Krivo, A.; Mirvoda, S. The Experience of Cyberthreats Analysis Using Business Intelligence System. In Proceedings of the 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 14–15 May 2020; pp. 0619–0622.
109. Mahmood, T.; Afzal, U. Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. In Proceedings of the 2013 2nd National Conference on Information Assurance (NCIA), Rawalpindi, Pakistan, 11–12 December 2013; pp. 129–134.
110. Anderson, R.; Moore, T. Information Security: Where Computer Science, Economics and Psychology Meet. *Philos. Trans. Math. Phys. Eng. Sci.* **2009**, *367*, 2717–2727. [CrossRef] [PubMed]
111. Varian, H. System reliability and free riding. In *Economics of Information Security*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 1–15.
112. Hausken, K. Information sharing among firms and cyber attacks. *J. Account. Public Policy* **2007**, *26*, 639–688. [CrossRef]
113. Moore, T. The economics of cybersecurity: Principles and policy options. *Int. J. Crit. Infrastruct. Prot.* **2010**, *3*, 103–117. [CrossRef]
114. Bauer, J.M.; Van Eeten, M.J. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommun. Policy* **2009**, *33*, 706–719. [CrossRef]
115. Lelarge, M.; Bolot, J. Economic incentives to increase security in the internet: The case for insurance. In Proceedings of the IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1494–1502.

116. Dacus, C.; Yannakogeorgos, P.A. Designing Cybersecurity into Defense Systems: An Information Economics Approach. *IEEE Secur. Priv.* **2016**, *14*, 44–51. [CrossRef]
117. Brangetto, P.; Aubyn, M. Economic aspects of national cyber security strategies. *Proj. Rep. Annex.* **2015**, *1*, 9–16.
118. Newmeyer, K.P. Elements of national cybersecurity strategy for developing nations. *Natl. Cybersecur. Inst. J.* **2015**, *1*, 9–19.
119. Kelly, D. The economics of cybersecurity. In Proceedings of the International Conference on Cyber Warfare and Security, Dayton, OH, USA, 2–3 March 2017; p. 522.
120. Massacci, F.; Ruprai, R.; Collinson, M.; Williams, J. Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers. *IEEE Secur. Priv.* **2016**, *14*, 52–60. [CrossRef]
121. Wong, G.; Greenhalgh, T.; Westhorp, G.; Buckingham, J.; Pawson, R. RAMESES publication standards: Meta-narrative reviews. *J. Adv. Nurs.* **2013**, *69*, 987–1004. [CrossRef]
122. Montuori, A. The complexity of transdisciplinary literature reviews. *Complicity Int. J. Complex. Educ.* **2013**, *10*, 45–55. [CrossRef]
123. Gough, D. Meta-narrative and realist reviews: Guidance, rules, publication standards and quality appraisal. *BMC Med.* **2013**, *11*, 1–4. [CrossRef]
124. Garousi, V.; Felderer, M.; Mäntylä, M.V. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Inf. Softw. Technol.* **2019**, *106*, 101–121. [CrossRef]
125. Hsu, C.; Lee, J.N.; Straub, D.W. Institutional influences on information systems security innovations. *Inf. Syst. Res.* **2012**, *23*, 918–939. [CrossRef]
126. Feng, N.; Wang, H.J.; Li, M. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Inf. Sci.* **2014**, *256*, 57–73. [CrossRef]
127. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; Zhou, L. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *J. Account. Public Policy* **2015**, *34*, 509–519. [CrossRef]
128. Jalali, M.S.; Siegel, M.; Madnick, S. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *J. Strateg. Inf. Syst.* **2019**, *28*, 66–82. [CrossRef]
129. Zhao, X.; Xue, L.; Whinston, A.B. Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *J. Manag. Inf. Syst.* **2013**, *30*, 123–152. [CrossRef]
130. Shetty, N.; Schwartz, G.; Felegyhazi, M.; Walrand, J. Competitive cyber-insurance and internet security. In *Economics of Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 229–247.
131. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W.; Zhou, L. Increasing cybersecurity investments in private sector firms. *J. Cybersecur.* **2015**, *1*, 3–17. [CrossRef]
132. Shackelford, S.J. Should your firm invest in cyber risk insurance? *Bus. Horiz.* **2012**, *55*, 349–356. [CrossRef]
133. Hausken, K. Returns to information security investment: Endogenizing the expected loss. *Inf. Syst. Front.* **2014**, *16*, 329–336. [CrossRef]
134. Gao, X.; Zhong, W.; Mei, S. Security investment and information sharing under an alternative security breach probability function. *Inf. Syst. Front.* **2015**, *17*, 423–438. [CrossRef]
135. Campbell, K.; Gordon, L.A.; Loeb, M.P.; Zhou, L. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *J. Comput. Secur.* **2003**, *11*, 431–448. [CrossRef]
136. Grossklags, J.; Christin, N.; Chuang, J. Secure or insure? A game-theoretic analysis of information security games. In Proceedings of the 17th International Conference on World Wide Web, Beijing, China, 21–25 April 2008; pp. 209–218.
137. Srinidhi, B.; Yan, J.; Tayi, G.K. Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decis. Support Syst.* **2015**, *75*, 49–62. [CrossRef]
138. Anderson, R.; Barton, C.; Böhme, R.; Clayton, R.; Van Eeten, M.J.; Levi, M.; Moore, T.; Savage, S. Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 265–300.
139. Cook, I.; Pfleeger, S. Security decision support challenges in data collection and use. *IEEE Secur. Priv.* **2010**, *8*, 28–35. [CrossRef]
140. Vishik, C.; Sheldon, F.; Ott, D. Economic incentives for cybersecurity: Using economics to design technologies ready for deployment. In *ISSE 2013 Securing Electronic Business Processes*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 133–147.
141. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W. Sharing information on computer systems security: An economic analysis. *J. Account. Public Policy* **2003**, *22*, 461–485. [CrossRef]
142. Rashid, Z.; Noor, U.; Altmann, J. Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. *Future Gener. Comput. Syst.* **2021**, *124*, 436–466. [CrossRef]
143. Rothman, K.J.; Greenland, S.; Lash, T.L. *Modern Epidemiology*; Lippincott Williams & Wilkins: Baltimore, MD, USA, 2008.
144. Caplin, A.; Schotter, A. *The Foundations of Positive and Normative Economics: A Handbook*; Oxford University Press: Oxford, UK, 2008.
145. Marotta, A.; Martinelli, F.; Nanni, S.; Orlando, A.; Yautsiukhin, A. Cyber-insurance survey. *Comput. Sci. Rev.* **2017**, *24*, 35–61. [CrossRef]
146. Samuelson, P.A. The pure theory of public expenditure. *Rev. Econ. Stat.* **1954**, *36*, 387–389. [CrossRef]
147. Mulligan, D.K.; Schneider, F.B. Doctrine for cybersecurity. *Daedalus* **2011**, *140*, 70–92. [CrossRef]
148. Asllani, A.; White, C.S.; Ettkin, L. Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. *J. Leg. Ethical Regul. Issues* **2013**, *16*, 7.

149. Rietveld, J.; Schilling, M.A. Platform competition: A systematic and interdisciplinary review of the literature. *J. Manag.* **2021**, *47*, 0149206320969791. [CrossRef]
150. Al Sabbagh, B.; Kowalski, S. A socio-technical framework for threat modeling a software supply chain. *IEEE Secur. Priv.* **2015**, *13*, 30–39. [CrossRef]
151. Vagle, J.L. Cybersecurity and Moral Hazard. *Stanf. Tech. Law Rev.* **2020**, *23*, 71. [CrossRef]
152. Brito, J.; Watkins, T. Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy. *Harard Natl. Secur. J.* **2011**, *3*, 39.
153. Anderson, R.; Barton, C.; Bölme, R.; Clayton, R.; Ganán, C.; Grasso, T.; Levi, M.; Moore, T.; Vasek, M. Measuring the Changing Cost of Cybercrime. In Proceedings of the 18th Annual Workshop on the Economics of Information Security, Boston, MA, USA, 3–4 June 2019.
154. Kumar, R.; Baz, A.; Alhakami, H.; Alhakami, W.; Agrawal, A.; Khan, R.A. A hybrid fuzzy rule-based multi-criteria framework for sustainable-security assessment of web application. *Ain Shams Eng. J.* **2021**, *12*, 2227–2240. [CrossRef]
155. Thurner, S.; Poledna, S. DebtRank-transparency: Controlling systemic risk in financial networks. *Sci. Rep.* **2013**, *3*, 1888. [CrossRef]
156. Ahmadi, E.; McLellan, B.; Tezuka, T. The economic synergies of modelling the renewable energy-water nexus towards sustainability. *Renew. Energy* **2020**, *162*, 1347–1366. [CrossRef]
157. Barabási, A.L.; Gulbahce, N.; Loscalzo, J. Network medicine: A network-based approach to human disease. *Nat. Rev. Genet.* **2011**, *12*, 56–68. [CrossRef]
158. Morgan, S. *2019 Official Annual Cybercrime Report*; Technical Report; Cybersecurity Ventures: Northport, NY, USA, 2020.
159. Moore, T.; Kenneally, E.; Collett, M.; Thapa, P. Valuing Cybersecurity Research Datasets. In Proceedings of the 18th Workshop on the Economics of Information Security (WEIS), Boston, MA, USA, 3–4 June 2019.
160. Corti, L.; Van den Eynden, V.; Bishop, L.; Woollard, M. *Managing and Sharing Research Data: A Guide to Good Practice*; Sage: Newcastle upon Tyne, UK, 2019.
161. March, S.T.; Smith, G.F. Design and natural science research on information technology. *Decis. Support Syst.* **1995**, *15*, 251–266. [CrossRef]
162. Kianpour, M.; Kowalski, S.J.; Øverby, H. Multi-Paradigmatic Approaches in Cybersecurity Economics. In Proceedings of the STPIS’21: Workshop on Socio-Technical Perspectives in Information Systems, Trento, Italy, 14–15 October 2021.