Trim, Peter R.J. and Lee, Y.-I. (2021) The global cyber security model: counteracting cyber attacks through a resilient partnership arrangement. Big Data and Cognitive Computing 5 (3), e32. ISSN 2504-2289.

big data and cognitive computing

MDPI

Article

The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement

Peter R.J. Trim [1,*] and Yang-Im Lee [2]

[1] Department of Management, School of Business, Economics and Informatics, Birkbeck, University of London, Malet Street, London WC1E 7HX, UK
[2] Department of Marketing & Business Strategy, Westminster Business School, University of Westminster, 35 Marylebone Road, London NW1 5LS, UK; y.lee@westminster.ac.uk
* Correspondence: p.trim@bbk.ac.uk; Tel.: +44-0207-631-6764; Fax: +44-0207-631-6769

Abstract: In this paper, insights are provided into how senior managers can establish a global cyber security model that raises cyber security awareness among staff in a partnership arrangement and ensures that cyber attacks are anticipated and dealt with in real time. We deployed a qualitative research strategy that involved a group interview involving cyber security and intelligence experts. The coding approach was used to identify the themes in the data and, in addition, a number of categories and subcategories were identified. The mind map approach was utilized to identify the thought processes of senior managers in relation to ensuring that the cyber security management process is effective. The global cyber security model can be used by senior managers to establish a framework for dealing with a range of cyber security attacks, as well as to upgrade the cyber security skill and knowledge base of individuals. In order for a cyber security mentality to be established, senior managers need to ensure that staff are focused on organizational vulnerability and resilience, there is an open and transparent communication process in place, and staff are committed to sharing cyber security knowledge. By placing cyber security within the context of a partnership arrangement, senior managers can adopt a collectivist approach to cyber security and benefit from the knowledge of external experts.

Keywords: awareness; cyber security; intelligence; partnership arrangement; resilience

Citation: Trim, P.R.J.; Lee, Y.-I. The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement. *Big Data Cogn. Comput.* **2021**, *5*, 32. https://doi.org/10.3390/bdcc5030032

Academic Editor: Min Chen

Received: 26 May 2021
Accepted: 8 July 2021
Published: 13 July 2021

1. Introduction

In the past, practitioners and researchers from various fields have invested time and effort into establishing robust cyber security models, frameworks, and approaches that staff within organizations can use to counteract the actions of cyber criminals. They have been diverse in orientation and in some cases have been inter-disciplinary or multi-disciplinary in nature. However, to some degree, they have been constrained in terms of their application. In addition, security issues tend to be the priority of designated experts within an organization. This is understandable in the sense that the subject matter covered can be considered computer and information technology and systems oriented, as well as highly specialized.

Those involved in the various aspects of cyber security and policy understand that defending society against cyber attacks needs to be viewed from an international perspective as opposed to a national perspective. Cyber attacks are increasingly becoming more sophisticated and the damage caused is becoming of economic concern. There is recognition that cyber attacks are becoming better coordinated and more sophisticated, and as people's lifestyle changes through the use of technology, the intensity of attacks is expected to increase. For example, according to the World Economic Forum, the annual cost of cyber crime is estimated to be US$445 billion [1] (p. 2).

Organizations that have been hacked and had large amounts of confidential data stolen have not always responded to the challenge in the way expected. In some cases, small

companies have been made bankrupt by hackers emptying their accounts of funds. The ransomware attack in May 2021 on the Colonial Pipeline in the USA [2] suggests that those carrying out such an attack study the target organization carefully in advance so that they know how to maximize their gain. Attacks on private and not-for-profit organizations, and on critical national infrastructure and critical information infrastructure, are of concern to policy makers. This moves the debate from the actions of cyber criminals to those engaged in cyber warfare and cyber terrorism. It is for this reason that a broader view of the use of cyber security models is needed. Hence, managers in organizations need to adopt a more pro-active approach to cyber security and its management, which includes broadening the skills and knowledge base of employees so they are better able to deal with cyber attacks in real time. The question that arises is, how can senior managers within an organization devise a comprehensive cyber security strategy that incorporates cyber security skill and knowledge enhancement to ensure that the organization is resilient? From the perspective of the authors of this paper, resilience is viewed in terms of an organization and its partners, as opposed to a single organization. A partnership arrangement includes all the organizations in the firm's network ranging from the suppliers at one end of the spectrum through to those in the marketing channel on the other end. It can be suggested, therefore, that a collectivist approach to cyber security is needed so that an inter-organizational coordinated response materializes.

In order to reduce the harmful effect, such as physical or digital, economic, psychological, reputational, social, and societal factors [3], it is necessary to understand that the nature of cyber attacks varies and is ongoing. Hence, senior managers need to motivate staff as well as increase the organization's resilience. Attention needs to be given to anticipating and preventing a cyber attack from penetrating an organization's defences. Reputational damage to an organization can result in a decreased share price, or it can cause customers to disassociate themselves from the organization and engage in business with a competitor for example. It is with this in mind that the authors of this paper explain how managers within an organization can counteract the threat of cyber attacks. In doing so, we develop a conceptual model that shows which aspects senior managers need to pay attention to and how they should coordinate various cyber security actions through sharing information with partner organizations that results in the utilization of cyber security knowledge.

The outcome of the research highlights the fact that the computer systems and networks in place need to be expertly managed and updated through time as this will help staff to diagnose problems and place the knowledge gained in the organization's memory. Naturally, this draws out the importance of staff reflecting on their past experience and identifying shortcomings in their skill and knowledge to respond effectively to a range of cyber attacks in real time. This reinforces the importance of prioritizing supply chain vulnerabilities, as it is organizations in the supply chain that are likely to be the weakest link in the network. By establishing a cyber security ethos that promotes learning and self development, the cyber security skill and knowledge base of staff throughout the partnership arrangement will be raised.

The paper was structured in the following way. First, attention is given to the post-COVID-19 era and big data, and this is followed by learning and cyber security knowledge development. Next, a section entitled cyber security models is provided and is followed by a section entitled interactive behaviour and managing change. After the methodology section, the findings and discussion are followed by a section entitled the global cyber security (GCS) model. The paper ends with a conclusion.

2. The Post-COVID-19 Era and Big Data

The COVID-19 pandemic has affected organizations in a number of ways such as remote working, connectivity, and security. Sharma, Adhikary, and Borah [4] (p. 444) have indicated that demand uncertainty, security breaches, and a resilient supply chain are key concerns managers are dealing with at present. To meet the rapidly increasing demand for Internet connectivity and service provision, organizations are undergoing digital

transformation, which may present a problem for some partner organizations. To ensure that an organization is not vulnerable to a cyber attack, staff throughout the partnership arrangement need to be involved in risk management and establish an integrated risk management process. Furthermore, senior managers should also be aware of how staff in the various business functions deal with what can be described as a proliferation of data, bearing in mind that artificial intelligence (AI) tools can be utilized to analyze and interpret large data sets, but not every organization has access to such tools. In addition, there is the issue of the standardization and unification of data, and interoperability. If staff do not know how to interpret the data analyzed through AI, and remote working results in inadequate communication between staff, it is likely that the organization will become vulnerable. As a consequence, managers are less able to deal with or respond to a problem in real time.

Taking into account the issue of big data proliferation, McAfee and Brynjolfsson [5] (p. 4) indicate that big data represents "messages, updates, and images posted on social networks; readings from censors; GPS signals from cell phones, and more". It is not surprising to learn, therefore, that the structured corporate data bases that store such data and process it may not always be appropriate [5] (p. 5) because computer systems are updated in different ways; Payraudeau, Dencik, and Marshall [6] (p. 19) are clear that managers need to think in terms of building an enterprise-wide security strategy if they are to have effective counter measures in place. This means improving the security of applications and data, staff being compliant and acknowledging data privacy regulations, and compliance being enabled in terms of enterprise security policies [6] (p. 19).

What has to be remembered is that there are different sources of data. There are public data (e.g., data held and derived from government, government organizations, and local communities); private data (e.g., data held and derived from private companies, not-for-profit organizations, and individuals); data exhaust (e.g., data of a general nature that are collected and have limited value); community data (e.g., data distilled into social tends); and self-quantification data (e.g., data that result from quantifiable personal actions or behaviour) [7] (p. 322). There are a number of methods that can be used for analyzing big data sets and managers need to be aware of what they are looking for in the data. General data that are deficient in some way are not as appropriate as defined, reliable data known to be recurring. High quality data, as defined by the user, can be analyzed so that the patterns in the data yield insights into a particular phenomenon. This can also be done by algorithms in the sense that machine learning involves computers learning to classify information and recognize patterns in the data without being programmed to do so [8] (p. 2). AI tools exist to help managers undertake a quantitative analysis, which is undertaken in order to establish cause and effect or truth; and a qualitative analysis, whereby the patterns in the data are uncovered and result in the discovery of something new or something that is emerging. AI has the ability, therefore, to help in the analysis and planning of marketing strategies and the analysis and interpretation of threat data. This suggests that AI can help managers to coordinate the knowledge development process across business functions.

Prior to data usage, it is important for those involved in cyber security to understand how they are to clean the data because, even if they are working with known AI tools, they need to be able to spot if something is an isolated event or recurring. Data processing is the first stage of the data mining operation and is undertaken in order to remove noise and data inconsistencies, and ensure that only the relevant data are selected [8] (p. 7). Hence, in the post-processing period, patterns in the data are evaluated and the knowledge is visualized and presented for analysis [8] (p. 8). However, although innovative organizations are known to embrace the use of data, the role of a chief information officer is important in terms of ensuring the availability of data and the infrastructure that supports the flow of data, as well as the trust and transparency of the data in the context of what data can be shared [9] (p. 4).

The more interconnected companies are in terms of working on joint projects and sharing costs, facilities, and manpower, the more they will need to be committed to undertake risk assessments on a regular basis. Hence, senior managers need to establish how risk will be managed among the partner organizations. By establishing a risk management policy among partner organizations, staff will be able to share quality data and information, and deploy appropriate risk analysis tools.

3. Learning and Cyber Security Knowledge Development

Humerick [10] (p. 395) suggests that artificial intelligence will become more influential in the years ahead as staff collect large amounts of personal data from customers and algorithms learn, and thus help managers to make informed decisions. However, the GDPR (general data protection regulation), governed by the European Union, forces member states to ensure that those that collect, store, and utilize customer data do so within strict limits because the consumer has specific rights [10] (p. 396). Indeed, the main objective of regulators is to make sure that the security systems in place safeguard the data belonging to consumers and, as a consequence, consumers are not put at risk. Should a data breach occur, it may result in multiple cases of identity theft, which can be attributed to two problems: inadequate privy protection and insufficient data security [11] (p. 443). This calls into question the role of the chief information officer and what form of governance mechanism there is in place.

In order to establish an effective learning model, senior managers need to identify the skill and knowledge gaps that exist and keep staff motivated so that they maintain their cyber security awareness. Increasing awareness is necessary as those that carry out cyber attacks are becoming more focused on exploiting known vulnerabilities, but equally, they indulge in opportunistic behaviour in order to find new targets on which to focus their efforts. Senior managers may invest in the latest computer and network security and deploy sensors in the network(s) so that when an attack is detected, appropriate staff are alerted. What needs to be remembered is that security still rests with individuals who need to detect, report, and monitor intrusions. By investing in appropriate, up-to-date cyber security training programmes and having in place an internal cyber security awareness campaign, human error can be reduced and confidential data and information can be protected. In addition, by investing in blockchain technology, staff based in a partnership arrangement can benefit from sharing threat information and thus counteract future cyber attacks [12] (p. 10). This reiterates the point relating to the organization's memory as staff must be able to turn information (e.g., attacks, impacts, and outcomes) into knowledge and transfer the knowledge through the shared learning model that is in existence.

Strauß [13] (pp. 6–7) is right to highlight the ethical concerns related to AI and, further, managers need to be aware of the problems linked with the risk associated with computer-generated outcomes. For example, Hagendorff and Wezel [14] (p. 356) suggest that datasets can be biased or faked or falsified. It is for this reason that senior managers need to understand what AI is required to deliver in terms of the capability of staff. If an AI system is designed inappropriately, and staff are not able to understand how the deep learning involved gives rise to the results that are evident, it could be that the AI policy in place is flawed. One reason this may occur is because staff are not aware of (i) what the cyber security systems in place are supposed to achieve and (ii) how to interpret the AI outcome. If there is a mismatch in the design of the system and the ability of managers to understand and implement cyber security policy, the organization is vulnerable to an attack. Should this be the case, staff will need to undergo cyber security awareness training and develop a better understanding of how to utilize AI to detect threats. Bearing in mind that the objective is to improve cyber security throughout the partnership arrangement, it can be deduced that the cyber security awareness programme in place needs to be hosted in a collectivist manner as the risk associated with a cyber attack is viewed as a shared responsibility and not an individual company's responsibility.

4. Cyber Security Models

Various types of cyber security models have been developed over the years and it is interesting to note that they have covered a number of fields of enquiry and various industries, and have been of a quantitative or conceptual nature. In addition, the modelling process used has been linked to various threat environments so that managers can gain in-depth knowledge of the various types of security knowledge specific to computer networks and information systems. On the other hand, the modelling approach has been holistic and social science oriented and revolves around people and their interaction in the work environment. According to Le and Hoang [15] (p. 1), cyber security is interpreted differently by staff and, because of this, they offer the following definition [15] (p. 3): "Cyber security can be considered systems, tools, processes, practices, concepts and strategies to prevent and protect the cyber space from unauthorized interaction by agents with elements of the space to maintain and preserve the confidentiality, integrity, availability, and other properties of the space and its protected resources".

The capability maturity model by Humphrey [15] (p. 4) has proved useful as it has made software developers aware of the need to develop software quality through a continual process of development, and ultimately, the goal is achievement and capability. Since then, the developers of such models have taken cognizance of the various international standards that have been devised and that offer guidance and hold managers accountable through compliance. Some of the auditing tools associated with such models are available via specialist consultancy providers and they update the user in terms of the requirements of international standards. Le and Hoang [15] (p. 6) raise a pertinent point by suggesting that such models are used both by management and security experts to establish the security status of the organization. By hiring security specialists, managers can utilize expert knowledge and develop contingency plans as necessary.

The sequence-of-events model [16] (pp. 33–36) can be used by managers to evaluate the cyber security threats in the market and identify and prioritize actions and responses in relation to cyber crime, cyber warfare, and cyber terrorism. A generic cyber security management model [16] (pp. 201–202), which again is conceptual in nature and links the organization's internal and external environments, has an education and training component and can help managers develop a cyber security policy that is supportive of a defined cyber security strategy. Furthermore, the modified and extended generic cyber security management model, which incorporates a software tool that monitors sensor activity in computer networks, provides a strategic framework within which specific managers are informed that an attack on the organization is underway [16] (p. 202).

Cotae, Kang, and Velazquez [17] have adopted a different approach to cyber security by utilizing game theory and the decision-making process. The cybersecurity optimal decision-making model or cybergame model they have developed is focused on perceived damage and the cost in association with potential defensive action. It also takes into account the benefit to mission, and ensures that issues relating to risk and uncertainty are taken into consideration. The model is of interest to managers because it can be used as a basis for staff to learn about possible cyber attacks and how they impact the organization and, further, staff can devise defensive strategies that require them to adhere to organizational policy. It can be assumed that any skill- or knowledge-related deficiencies that surface during the use of the model will be highlighted and individual employees will be required to undertake a cyber security training programme and raise their cyber security skill base.

The factor analysis of information risk (FAIR) model is used for quantitative cyber security risk assessment and can help staff analyze interactions involving attackers and defenders [18] (p. 15). It is, however, viewed as rather restrictive. Notwithstanding, the FAIR model is well utilized and has done much to promote the concept of cyber security risk assessment within an organization. Attention has been given to cyber security resource allocation and, in particular, integrated risk analysis [19] does much to highlight the detail needed in a specific industry focused model. Underpinning this approach is adequate use of security controls and risk mitigation and the fact that an adequate model needs to be

formalized and comprehensive. For example, security portfolio and insurance are included by the authors and their model includes a whole range of threats.

Reflecting on modelling and its use, it is appropriate to suggest that, because cyber security does have different connotations and interpretations associated with it, a wide view of modelling relevant phenomena in relation to cyber security should be championed. Security, as a field of enquiry, is often detached from mainstream academic subjects. By adopting a widespread and inclusive approach to cyber security, it is possible to place emphasis on what Abou el Kalam [20] (p. 2) calls OM-AM holistic security concerning protecting supervisory control and data acquisition (SCADA) systems in the context of critical infrastructure. The four stage OM-AM (objective, model, architecture, and mechanism) approach offers a refreshing view of model construction in the sense that it allows the model builder to include an abstract level and a concrete level within it [20] (p. 7). For example, the role that an individual plays appears at the abstract level and the action they undertake appears at the concrete level. Bearing this in mind, it can be suggested that the influence an individual has on security (e.g., the chief information officer, the head of IT, and the risk manager) can be measured in terms of their inputs and outputs. Such an approach is deemed useful as it allows managers to better understand the threat landscape and how to develop a security culture, which equates cyber security awareness with cyber security training and educational provision. This leads to the current view of thinking purporting that cyber security education needs to include cyber ethics and, further, educators need to think in terms of developing ethical cyber theories [21]. The logic underpinning this view is that an interdisciplinary and inter-industry approach to cyber ethics education will help staff understand the range and nature of cyber attacks and the effect they have on society, and possibly the fact that a shared responsibility for the problem is required.

There are other models, such as the GISES (global intelligence and security environmental sustainability) model [22], (p. 456), which is of a conceptual nature and facilitates partnership development between industry and government and organizations in the public and private sectors. Conceptual models such as these can be drawn on because they have a security dimension, which can be applied in a cyber security context. The GISES model includes the following [22]: inputs (intelligence, security, and law enforcement objectives); issues (controllable and uncontrollable factors); policy (law enforcement, national security risk, and uncertainty assessment); influences (overseas government, international institutions, and international agencies); and outputs (intelligence and security upgraded). The model highlights the importance associated with learning and the knowledge development process concerning the sharing of information between parties in order to increase the level of security. Moreover, the model highlights the need for staff to be trained so that they are aware of environmental change relating to security issues and, in particular, how managers can establish intra- and inter-organizational support in terms of risk reduction.

5. Interactive Behaviour and Managing Change

Learning is linked with managing change and requires senior managers to adopt a risk reduction approach that allows staff to identify a potential threat and deal with it before it becomes an actual threat [23] (p. 184). It is for this reason that the learning model in place needs to be transparent and flexible. By adopting a pro-active approach to learning, it should be possible to view cyber security skill development from a number of organizational perspectives. The advantage of such an approach is that it provides a basis for institutionalizing learning and the development of knowledge. Hence, senior managers need to be fully engaged, as can be deduced from the following quotation [23] (p. 189): "The institutionalizing organizational learning process is very complex and needs to be managed strategically if that is, the resources devoted to training and staff development are to yield the returns expected".

In order to succeed at managing change, senior managers should understand that cyber security risks will both increase and decrease through time depending upon how

two sets of variables are managed: (i) controllable variables (management have perfect information and know what is involved); and (ii) uncontrollable variables (management have imperfect information and do not know what is involved). What emerges from this view is that the level of staff motivation in relation to counteracting cyber attacks will require behavioural change, which needs to be managed if appropriate working practices are to be created. This is because new business models are being developed that require new security skills, security knowledge, and an increased security capability. As organizations enter the new era of human–computer interaction and the use of AI increases, a new view of learning is required as change is rapid and dynamic.

5.1. Interactive Behaviour and Cyber Security Awareness

Artificial intelligence provides a new way for staff to interact with customers and think less about how technology works and more about how to utilize the results. What senior managers need to realize is that, because the term cyber can be deployed quite widely, it is essential for employees to be grounded in cyber business practices and develop a corresponding cyber security mindset. Should this be the case, it is likely that those lower down the hierarchy will be able to think in terms of integrating the organization's strategic intelligence, planning, and implementation process within a cyber security framework. The main advantage of this is that it will raise the profile of security throughout the organization and ensure that cyber security is embraced and not feared (e.g., surveillance is there to protect an asset and not harm or disrupt it). The interactive behavioural cyber security awareness process and the thinking behind it appear in Figure 1.

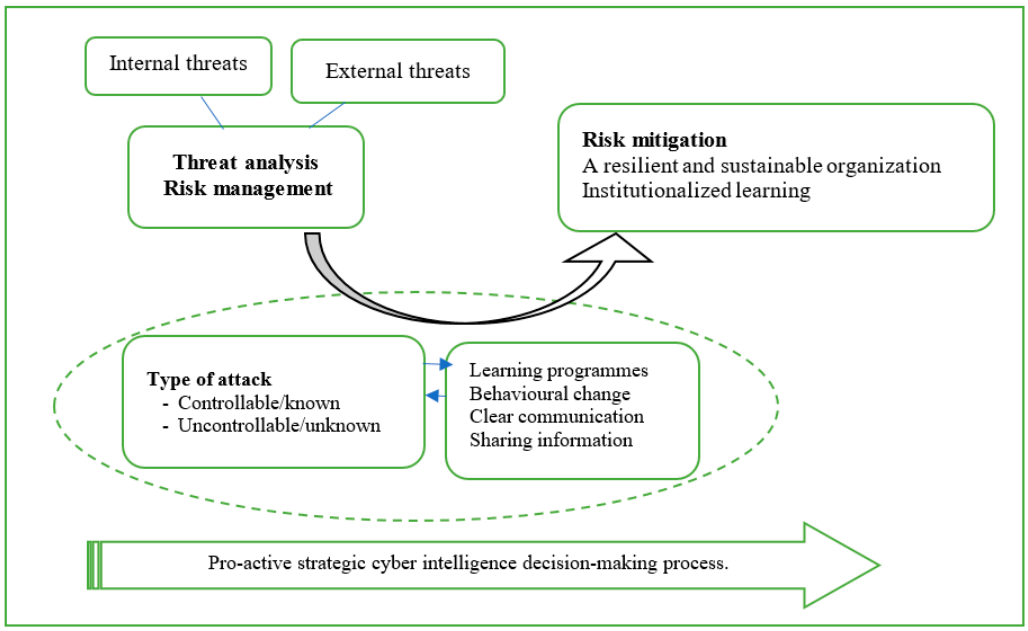

Figure 1. The interactive behavioural cyber security awareness process.

Reflecting on Figure 1, it can be suggested that learning should be viewed as helping managers to develop and raise the cyber security skill base of staff throughout the partnership arrangement and develop staff awareness in terms of the uncontrollable and unknown cyber security attacks. By placing learning within a pro-active strategic cyber intelligence decision-making process, a cyber security management strategy can be developed that has risk mitigation at its centre. For example, by understanding how employees absorb information and knowledge while undertaking intelligence and planning activities, cyber security training programmes can be devised that increase the strategic skill base of employees. This should enable staff to deal with the full range of cyber attacks and liaise with staff who deal with computers and information technology. By developing a collectivist security

culture, both the internal and external strategic decision-making process will be extended to include all the business functions. The key point to note is that risk assessment and risk analysis need to be viewed as a shared responsibility. Therefore, in-house staff should work with staff in partner organizations to produce an inter-company, integrated security mechanism that is monitored and managed by the organization's risk manager or a risk committee (formed from various managers and overseen by the chief information officer). This should facilitate strategic intelligence decision-making throughout the partnership arrangement so that the outcome associated with the uncontrollable variables can be dealt with in a pro-active and timely manner.

What is evident from the discussions above is that senior managers can use the learning approach to share information and knowledge relating to cyber incidents and promote cyber security awareness. Various researchers [24,25] have contributed to the topic of cyber security awareness by providing insights into how senior managers can view cyber security behavioural awareness and improve cyber security among staff to make the organization more resilient. To facilitate information sharing and knowledge transfer within and between partner organizations, it is necessary to adopt an open style of communication. An open style of communication is viewed as reinforcing an organization's learning culture and should allow information sharing that results in new knowledge being produced [26]. Through sharing strategic intelligence and fostering a learning model that is relevant to the industry in which the organization competes, staff in partner organizations can adopt a pro-active, adaptive, and risk sharing approach to cyber security.

During the knowledge development process, staff also interact with individuals external to the organization, and this results in the convergence of knowledge [27,28]. Through the knowledge sharing process, emotional bonds are formed that give rise to a set of relationships that allow information/knowledge to be exchanged, and this enhances the group's knowledge [29]. An important observation that can be made is that, by having a clear idea of which relationships to invest in and what the level of commitment is, it makes it easier for an employee to develop relationships that promote the concept of mutuality. For example, it has been suggested that, by adopting a more focused view as to what strategic intelligence represents, it will be easier for senior managers to think in terms of making the organization more resilient [30]. This suggests that managers should develop a cyber security management framework that incorporates governance, risk, and compliance [16].

5.2. Partnership Arrangements in Context

It is useful to note that arrangements with partner organizations evolve through time and so do the governance mechanisms that hold senior managers to account. Governance helps managers to integrate the various decision-making processes by focusing attention on uncontrollable threat variables and establishing appropriate risk mitigation. Hence, senior managers need to define what a partnership arrangement represents as the concept of mutuality suggests that the cultural value systems of the partner organizations are in unison. A partnership arrangement can be defined as follows [31] (p. 223): "An all embracing mutually oriented mechanism that allows staff within an organization to identify, devise and implement a legal instrument that results in combined ownership, an integrated management model that is underpinned by a hybrid organizational culture, which gives rise to a clearly defined mission statement and marketing strategy".

Reflecting on an organization's vulnerability, it is suggested that there are several ways to reduce an organization's level of risk [32]. One way is to identify and select trustworthy business partners that avoid opportunistic behaviour. This supports the argument for a collectivist approach to security that incorporates intelligence focused strategic decision making. By ensuring that each organization in the partnership arrangement has a recognizable mission statement that is underpinned by a logical and proven set of values, it is possible to ensure that trust is maintained within the organization and between organizations. Trust can be viewed from two perspectives. First, trust can be perceived as

credibility (which refers to the ability to perform a given task satisfactorily); and second, it can be viewed as benevolence (which requires that short-term benefits are given-up for a long-term relationship and mutual benefits). This suggests that trust is a pivotal element in the strategy process when two or more organizations attempt to build a strong, continuous relationship. The relevance of this can be seen in the context of buyer–supplier relationships and how managers devise an appropriate cyber supply chain risk management system [33] that results in risks being adequately assessed and contingencies put in place to deal with unseen impositions.

Taking into account the discussions above, five questions emerge:

Question 1: How can senior managers devise a strategic partnership arrangement that is reinforced by individual partners that have a robust cyber security strategy in place?
Question 2: How can senior managers ensure that the concept of mutuality prevails and manifests in a co-owned cyber security strategy that is sustainable throughout the partnership arrangement?
Question 3: How can senior managers continually promote the concept of organizational learning so that the inter-relationships within the strategic partnership arrangement are known to be trustworthy?
Question 4: How can the resilience of a strategic partnership arrangement be maintained?
Question 5: What form of governance mechanism can senior managers implement in order to ensure that the co-owned cyber security strategy is sustainable through time?

6. Methodology

Reflecting on the forgoing discussions, and bearing in mind the open-ended questions that emerged, it was decided that a qualitative research strategy would be adopted involving a group interview and a two-step analytical approach (coding [34] and mind mapping [35]), so the researchers could answer the following question: how can senior managers within an organization devise a comprehensive cyber security strategy that incorporates cyber security skill and knowledge enhancement to ensure that the organization is resilient? For this study, we used the group interview method as the subject matter was of a complex nature. The research method allowed us to gain insights from cyber security and intelligence specialists into the real world of managing cyber security threats in an organizational setting. Initially, it was hoped that forty intelligence and security experts, all of whom had wide industry experience, would participate in the research project, as this would have allowed two group interviews to be undertaken. However, it became clear after several months that fewer people were willing to participate in the study because of a number of factors (e.g., timing and work commitments). Those that did participate in the study applied for and were given permission to participate in a group interview.

All twenty senior cyber security and intelligence experts that agreed to take part in the group interview had extensive industry experience. The group interview method was chosen because it allows participants to share their experiences and engage in interpretation and challenge the thoughts of others [36]. Those that participated in the group interview did not want their identify or indeed the identity of their organization to be made public and a strict code of ethical practice was adhered to. In order to ensure that a participant's identity was not revealed, the group interview was not audio-recorded; however, the researchers took copious notes during the group interview and compared their findings after they had completed their write-up.

During the group interview, a number of open-ended questions were posed and further questions proved valuable in terms of probing [36]. On occasion, however, when the subject matter became sensitive and a participant felt uncomfortable, the line of enquiry was changed so that the wider issues under consideration could be discussed further. This maintained the commitment of the participants and avoided the group interview being terminated early as there were no grounds to do so. The group interview consumed half a day and yielded a great deal of data. The topics covered included the following: interdependence throughout the supply chain and the marketing channel; organizational

vulnerability in the context of a partnership arrangement; the way senior management put in place structures and procedures that protected the organization against a possible cyber attack; and how organizational staff should work with external stakeholders in terms of both imparting information about a cyber attack and receiving information as to how they can deal with or limit a specific type of cyber attack. The discussions branched out and focused mainly on current and future security skill gaps; how to establish and put in place an organization specific security culture that has at its centre a focus on cyber security; and the way in which to manage inter-organizational relationships so that trust is ensured and sensitive data and information is exchanged in real time.

The coding process [34] was used to identify the themes that emerged from the group interview and the process was complete once the third-order themes were realized. Indeed, the coding approach, whereby labels were assigned to phrases spoken by the participants, allowed the researchers to link the themes identified and establish the main categories and establish how the subcategories were linked to the main categories. This provided conceptual density [34]. By identifying the key themes and the links between each of the themes identified [37], the researchers could establish how and why the participants communicated in the way that they did [38]. In addition, the researchers were able to develop a holistic view of security within an organization and better understand how security personnel utilize knowledge and ensure that a security culture is established and permeates throughout a partnership arrangement.

The second stage of the analysis involved mind mapping and this was done in order to establish the inner thought processes [35] of the cyber security and intelligence experts. For example, one of the areas addressed was to establish who in an organization is responsible for security. It is known that senior management teams have a different view of security depending upon the industry in which they operate. It can also be suggested that organizations that do not have a chief information officer in place are likely to be less strategically focused and rely on a risk manager for complying with government regulations. Therefore, it was necessary to establish if security was to be identified as a cross-organizational prerogative or if it was focused more on computer and information technology (IT). Of key interest was establishing if staff in IT had authority to take responsibility for both IT security and security in general or whether security was a divided responsibility. Other aspects that needed attention were the type of skill and background needed to understand and anticipate how cyber attacks would be launched on an organization and the way in which attacks could be dealt with in real time. The intellectual challenge was to establish how senior managers viewed cyber security evolving and how the envelope of security has widened so that IT security is viewed as central to the organization's sustainability. By getting inside the mindset of senior managers, it allowed the researchers to have a clearer appreciation of what constituted a cyber security counteractive threats framework and how such a framework would emerge.

7. Findings and Discussion

Taking into consideration the main research question, the mind mapping exercise produced (in simplified form) the information in Table 1.

The mind mapping exercise proved valuable in terms of providing evidence of how senior managers within an organization, who maybe struggling to put in place a cyber security management framework, can utilize the cyber security skill and knowledge base of partner organizations. Hence, when undertaking the mind map analysis, attention was given to how senior managers derive and make use of knowledge from outside the organization [28].

Table 1. Results of the mind mapping exercise.

Consensus View	Objective	Means/Solution
Staff are required to share information in real time.	To establish the type and nature of the threat/attack.	To utilize the knowledge and skill of expert staff.
Staff are required to communicate clearly.	To utilize cross-functional co-operation in real time.	To implement a risk mitigation plan to prevent cascading effects.
Inter-organizational co-operation is needed to thwart a cyber attack.	To reduce the impact on the organization and its partners in terms of share value and long-term financial position.	To exercise governance and ensure the organization is compliant.
Staff need to develop appropriate cyber security skills and knowledge.	To establish a minimum level of cyber security knowledge.	To implement cyber security training and education enhanced through cyber security awareness.

Through the coding process [34], five key themes were identified: (i) interdependence (e.g., inter-organizational co-operation is needed to thwart a cyber attack); (ii) security culture (e.g., staff are required to share information in real time); (iii) relationship building (e.g., staff are required to communicate clearly); (iv) organizational vulnerability (e.g., inadequate inter-organizational co-operation, inadequate sharing of information, poor communication, and insufficient cyber skills and knowledge); and (v) skill gaps (e.g., staff need to develop appropriate cyber security skills and knowledge). The reader will note that the themes were mapped against the consensus views in Table 1 and that, regarding theme (iv) organizational vulnerability, the contributing factors are an amalgamation of the other four themes relating to co-operation, information sharing, communication, and cyber skills and knowledge. Regarding Table 1, it is clear that organizational staff need to share relevant and sensitive information with staff in partner organizations and ensure that open communication manifests in cross-functional decision making. Non-disclosure agreements can be put in place to protect the parties involved. This view should result in a security culture and a co-owned cyber security strategy that is in place throughout the partnership arrangement. This being the case, the necessary contingency and emergency plans, once implemented, will help to harden the organization and make it more resilient. For example, cyber attacks that are launched on an organization/supply chain member will be dealt with in a specific way and may involve combined action from partner members. This is because the risk appetite is known and defined, and the perceived risk is shared. Agreements in place determine who in the partner organization takes responsibility for liaising with law enforcement personnel, for example. It can be argued that a cross-functional approach to cyber security management will result in senior managers being better informed regarding how they list the organization's risks in the risk register and how organizational staff communicate with external stakeholders. By monitoring cyber threats through a governance and compliance framework, it should be possible for staff to have better relations with government and regulatory bodies and industry associations, for example. What senior managers also need to realize is that the external environment is also a source of intelligence and managers throughout the partnership arrangement can prioritize the type of threat identified and communicate the possible threats to a wider audience via CERT-UK (U.K. national computer emergency response team), the Centre for the Protection of National Infrastructure (CPNI), or an industry association, for example. This is so that staff in a range of companies can quantify the cyber risk priorities identified. Hence, it is crucial for senior managers to ensure that there is a resilient network architecture in place and, further, that access management is effective [39].

By monitoring the external environment, it should be possible for senior managers to keep up with the trends in cyber crime and document the threats in the organization's risk register. By doing so, senior managers will be held accountable for investing in cy-

ber security training and educational programmes and, further, put in place appropriate management structures so that computer hackers do not exploit the partnership arrangement's vulnerabilities. If a coordinated approach to cyber security is not evident, then it may be necessary for the board of the organization to appoint a chief information security officer (CISO) [40] to oversee such a development and ensure adherence to the latest international standards.

In order for the organization to be made resilient and for the level of resilience to be maintained, it is necessary for senior managers to be transparent about the skill gaps that exist and how the necessary skills/expertise are to be brought into the organization and/or developed through time. One way to do this is to make sure that non-technical staff acquire the necessary level of IT knowledge and cyber security awareness so that they do not misuse a computer system (transfer data to an unknown person) and they know who to contact in times of a crisis. By ensuring that staff at different levels throughout the supply chain are trained to a high level of cyber security competency, the issue of technology handling should not be of major concern. If staff have an overarching view of cyber security and are knowledgeable in terms of how the organization's data travel through the company's networks, then it is likely they will be more responsive to how they deal with outsource partners and more able to visualize the problems associated with offshoring the organization's services. One way this can be done is by senior managers paying more attention to safeguarding information and ensuring that the information-centric approach is protected through managers conforming to the conditions laid out in international standards [41].

Reflecting on the relationship building aspect, it can be argued that senior management need to ensure that, in order for the security culture to be considered robust, the organization's human resources and management recruitment process, as well as those of its partner organizations (this also includes outsourcing companies), are robust in terms of the demands of current cyber security standards. Senior managers can view this from the perspective of due diligence and the need to make sure that, if staff undertake a certain organizational activity, they have the necessary security clearance. If an individual has not been trained in how to use a specific system and is not familiar with the security protocols that are in place, then it is possible that they will place the organization at risk. Furthermore, they may also place other members of the partnership arrangement at risk.

By viewing cyber security from a holistic perspective, it can be suggested that IT training and other forms of cyber security awareness training need to be put in place so that each employee gains from and is able to develop their technical skill and knowledge base. By establishing a security culture with a cyber heartland, it is possible to further develop the cyber security management processes and controls needed to make it effective. The advantage of this is that an appropriate risk management strategy can be developed that is co-owned by all the organizations within the partnership arrangement. Furthermore, bearing in mind that knowledge external to the organization is perceived as valuable, it is likely that open communication and information/knowledge exchange between staff in partner organizations will result in additional initiatives to counteract cyber attacks. Being open and sharing resources and avoiding conflict can be considered positive in terms of relationship building [42] and should be recommended.

The main argument being put forward is that open communication and a flexible approach to information/knowledge transfer will reinforce a cyber security culture that is underpinned by trust-based relationships and manifests in a co-owned cyber security framework and strategy. This is a key point to note because an organization's risk appetite can increase or decrease through time. Furthermore, because the external environment is undergoing rapid technologically induced change, senior managers may not know how vulnerable the organization is to various and specific forms of cyber attack. If a security breach does occur owing to a sophisticated attack getting through the organization's defence's, then it is likely that the cyber attack has penetrated the defences of the competitors.

Should this be the case, appropriate IT staff will liaise with the risk manager(s) and external law enforcement personnel.

8. The Global Cyber Security (GCS) Model

Reflecting on the results of the mind mapping exercise (Table 1), it can be suggested that, in order to develop cyber security awareness, senior managers need to be committed to establishing an organizational culture that is forward looking and pro-active in terms of embracing the use of technology. By placing cyber security at the centre of business operations, and having a governance mechanism in place, managers can adopt a responsible, but flexible approach to resilience. This should ensure that the key decision makers are able to deal with unexpected threats in a timely manner. Taking into account the above and placing it in the context of a conceptually oriented, social science cyber security model, it is possible to devise the global cyber security (GCS) model; please see Figure 2. The main focus of the model is to ensure that managers have a comprehensive understanding of what cyber security involves and the role that cyber security specialists play, as well as how managers can draw on intra- and inter-organizational support to reduce risk. The reader will note from Figure 2 that, in order for senior managers to establish a comprehensive cyber attack defence system, it is necessary to define what the organization's cyber security objectives are and to be realistic in terms of liaising with and requiring help from government representatives. Often, organizational staff are disappointed when they deal with government representatives because they provide information and data regarding a data breach and are not informed (owing to the nature of the intelligence led operation) as to how the investigation is carried out. An intelligence led operation involves both covert and overt operations and can run over many months. It is for this reason that senior managers need to establish what the controllable and uncontrollable factors are and what is necessary in terms of dealing with issues that have a national security dimension. The more borders the organization traverses, the more complex the security issue/problem becomes and, at times, staff are required to deal with law enforcement personnel from more than one country. However, because a cyber attack can be launched on an organization by hackers based overseas, the issue of physical barriers becomes less prominent and holding criminals accountable is a major obstacle to be overcome.

Drawing on in-house intelligence and reports relating to cyber attacks from a range of sources (government, private consultancies, and university research teams, for example), it should be possible for senior managers to identify, appraise, and prioritize cyber security risks and ensure that staff deal with them in real time. Through consultation with internal staff and external cyber security specialists, cyber security policy will be evaluated and the organization's cyber intelligence and security will be upgraded. This may mean that a strategy is adopted for AI, which is placed within the organization's learning model, and an alternative strategy is adopted for cloud computing, which is placed within computing and IT, for example.

From Figure 2, it can be noted that the cyber security steering group has an input into the organization's cyber security objectives and draws on the advice of domestic security specialists. An external group of cyber security advisors also provides information and intelligence that is used by senior managers and various lower management teams to set organizational security objectives. A range of cyber security specialists sit on the cyber attacks monitoring system committee, which is chaired by the chief information officer, and they are influential in terms of identifying how the separate organization's that make up the partnership arrangement utilize software in the form of sensors in the organization's networks. Multi-purpose sensors can be deployed that (i) collect consumer/customer oriented data and (ii) collect threat-related data. In addition, the cyber attacks monitoring system committee establishes and reviews cyber security training and educational programmes, as well as funds research into cyber security artificial intelligence. A key point to note is that relations with staff in university research departments that undertake projects in AI should

be fostered so that external advice can be drawn on when necessary and, further, students that specialize in AI can be recruited once they have completed their academic studies.

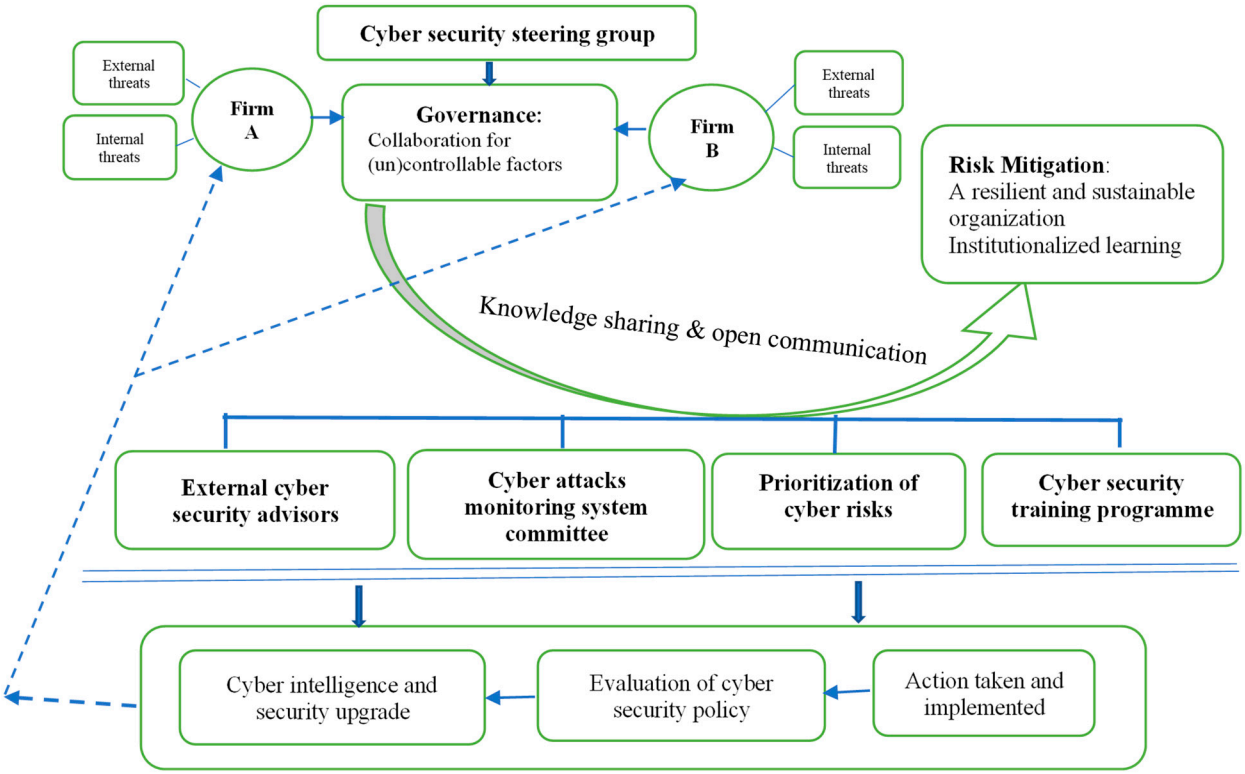

Figure 2. The global cyber security model.

9. Conclusions

This paper contributes to the area of cyber security awareness as it provides insights into why organizational structures and systems are interlinked and are used to enhance an organization's cyber security knowledge development. The global cyber security (GCS) model outlined helps managers visualize how they can establish and manage a strategy regarding risk mitigation concerning cyber security policy that makes the organization more resilient.

The way in which individuals form trust-based relationships can be considered important regarding their motivation to share information and turn information into knowledge [26,29]. There is no doubt that, in the years ahead, those charged with making sure the organization has a proper cyber security defence system in place will be required to draw on a range of external experts, some of whom are employed by university research departments and specialized research companies. This is because the level of cyber security knowledge needed and the type of cyber security knowledge required is beyond the capability of any single organization. What can be noted is that, by investing in cyber security awareness and providing the resources for the development of a cyber security model and approach, senior management should have a greater ability to harden the organization's cyber security defences and, at the same time, make the partnership arrangement more resilient.

In the years ahead, and taking into account the fact that the post-COVID-19 era has various unknowns associated with it, it is possible to suggest that organizational vulnerability is the main phenomenon that will concern intelligence and security experts, managers, and policy makers. In order for managers in organizations to fully understand the ramifications associated with cyber security, they need to think carefully about how an organization can derive the greatest benefit from the appointment of a chief information

officer and how a security culture with a cyber security heartland can be established. In addition, they need to look carefully at how the organization can derive an advantage from cyber security technology, AI, and specific types of models, so that a strategic cyber security decision-making process is adopted by managers throughout the partnership arrangement.

Author Contributions: Conceptualization, P.R.J.T. and Y.-I.L.; methodology, P.R.J.T. and Y.-I.L.; validation, P.R.J.T. and Y.-I.L.; formal analysis, P.R.J.T. and Y.-I.L.; investigation, P.R.J.T. and Y.-I.L.; writing—original draft preparation, P.R.J.T. and Y.-I.L.; writing—review and editing, P.R.J.T. and Y.-I.L. Both 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: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Restrictions apply to the availability of these data.

Acknowledgments: The authors would like to express their gratitude to the reviewers for their guidance and suggestions for improving the paper.

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

References

1. Vina, G. Patients in Limbo after Cyber Attack. *Financial Times*, 3 November 2016; p. 2.
2. Sanger, D.E.; Krauss, C.; Perlroth, N. Cyberattack Forces a Shutdown of a Top US Pipeline. Available online: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html (accessed on 13 July 2021).
3. Agrafiotis, I.; Nurse, J.R.C.; Goldsmith, M.; Cresse, S.; Upton, D.A. Taxonomy of Cyber-Harms: Defining Impacts of Cyber-Attacks and Understanding How They Propagate. *J. Cybersecur.* **2018**, *4*, 1–15. Available online: https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288?searchresult=1 (accessed on 19 May 2021). [CrossRef]
4. Sharma, A.; Adhikary, A.; Borah, S.B. Covid-19's Impact on Supply Chain Decisions: Strategic Insights from NASDAQ 100 Firms Using Twitter Data. *J. Bus. Res.* **2020**, *117*, 443–449. [CrossRef]
5. McAfee, A.; Brynjolfsson, E. Big Data: The Management Revolution. *Harvard Business Review*, 1 October 2012; pp. 1–9; Reprint R1210C.
6. Payraudeau, J.-S.; Dencik, J.; Marshall, A. *Digital Acceleration: Top Technologies Driving Growth in a Time of Crisis*; International Business Machines, Inc.: Armonk, NY, USA, 2020.
7. George, G.; Haas, M.; Pentland, A.S. From the Editors: Big Data and Management. *Acad. Manag. J.* **2014**, *57*, 321–326. [CrossRef]
8. Mink, D.M.; McDonald, J.; Bagui, S.; Glisson, W.B.; Shropshire, J.; Benton, R.; Russ, S. Near-Real-Time IDS for the U.S. FAA's NextGen ADS-B. *Big Data Cogn. Comput.* **2021**, *5*, 1–15.
9. IBM Institute for Business Value. *From Data Science to Data Diplomacy: Chief Information Officer Insights from the Global C-Suite Study*; IBM Corporation: Armonk, NY, USA, 2020.
10. Humerick, M. Taking AI Personally: How the E.U. must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence. *St. Clara High Technol. Law J.* **2018**, *34*, 393–418.
11. Jin, G.Z. Artificial Intelligence and Consumer Privacy. In *The Economics of Artificial Intelligence: An Agenda*; Agrawal, A., Gans, J., Goldfarb, A., Eds.; University of Chicago Press: Chicago, IL, USA, 2019; pp. 439–462.
12. Rawat, D.B.; Chaudhary, V.; Doku, R. Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems. *J. Cybersecur. Priv.* **2021**, *1*, 2. [CrossRef]
13. Strauß, S. Deep Automation Bias: How to Tackle a Wicked Problem of AI? *Big Data Cogn. Comput.* **2021**, *5*, 18. [CrossRef]
14. Hagendorff, T.; Wezel, K. 15 challenges for AI: Or What AI (Currently) Can't Do. *AI Soc.* **2019**, *35*, 355–365. [CrossRef]
15. Le, N.T.; Hoang, D.B. Can maturity models support cyber security? In Proceedings of the 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9–11 December 2016; IEEE: Piscataway, NJ, USA; pp. 1–7. [CrossRef]
16. Trim, P.R.J.; Lee, Y.-I. *Cyber Security Management: A Governance, Risk and Compliance Framework*; Gower Publishing: Farnham, UK, 2014.
17. Cotae, P.; Kang, M.; Velazquez, A. A Cybersecurity Model for Decision-Making Problems under Uncertainty Using Game Theory. In Proceedings of the 13th International Conference on Communications (COMM), Bucharest, Romania, 18–20 June 2020; IEEE: Piscataway, NJ, USA; pp. 15–22. [CrossRef]
18. Wang, J.; Neil, M.; Fenton, N. A Bayesian Network Approach for Cybersecurity Risk Assessment Implementing and Extending the FAIR Model. *Comput. Soc.* **2020**, *89*, 1–20. [CrossRef]
19. Insua, D.R.; Couce-Vieira, A.; Rubio, J.A.; Pieters, W.; Labunets, K.; Rasines, D.G. An Adversarial Risk Analysis Framework for Cybersecurity. *Risk Anal.* **2021**, *41*, 16–36. [CrossRef]
20. Abou el Kalam, A. Securing SCADA and Critical Industrial Systems: From Needs to Security Mechanisms. *Int. J. Crit. Infrastruct. Prot.* **2021**, *32*, 1–16. [CrossRef]

21. Petrie-Wyman, J.; Rodi, A.; McConnell, R. Why should I Behave? Addressing Unethical Cyber Behavior through Education. *Dev. Bus. Simul. Exp. Learn.* **2021**, *48*, 162–179.
22. Trim, P.R.J. The GISES Model for Counteracting Organized Crime and International Terrorism. *Int. J. Intell. Count.* **2005**, *18*, 451–472. [CrossRef]
23. Lee, Y.-I. Strategic Transformational Management in the Context of Inter-Organizational and Intra-Organizational Partnership Development. In *Strategizing Resilience and Reducing Vulnerability*; Trim, P.R.J., Caravelli, J., Eds.; Nova Science Publishers, Inc.: Hauppauge, NY, USA, 2009; pp. 181–196.
24. Trim, P.R.J.; Lee, Y.-I. The Role of B2B Marketers in Increasing Cyber Security Awareness and Influencing Behavioural Change. *Ind. Mark. Manag.* **2019**, *83*, 224–238. [CrossRef]
25. Kovačević, A.; Radenković, S.D. SAWIT-Security Awareness Improvement Tool in the Workplace. *Appl. Sci.* **2020**, *10*, 3065. [CrossRef]
26. Park, S.; Kim, E.J. Fostering Organizational Learning through Leadership and Knowledge Sharing. *J. Knowl. Manag.* **2018**, *22*, 1408–1423. [CrossRef]
27. Trim, P.R.J.; Upton, D. *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training*; Gower Publishing: Farnham, UK, 2013.
28. Nonaka, I.; Takeuchi, H. *The Knowledge-Creating Company*; Oxford University Press: Oxford, UK, 1995.
29. Oh, S.Y. Effects of Organizational Learning on Performance: The Moderating Roles of Trust in Leaders and Organizational Justice. *J. Knowl. Manag.* **2019**, *23*, 313–331. [CrossRef]
30. Trim, P.R.J.; Lee, Y.-I. A Strategic Marketing Intelligence and Multi-Organizational Resilience Framework. *Eur. J. Mark.* **2008**, *42*, 731–745. [CrossRef]
31. Trim, P.R.J.; Lee, Y.-I. A Strategic Approach to Sustainable Partnership Development. *Eur. Bus. Rev.* **2008**, *20*, 222–239. [CrossRef]
32. Sheffi, Y. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*; The MIT Press: Cambridge, MA, USA, 2005.
33. Boyson, S. Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems. *Technovation* **2014**, *34*, 342–353. [CrossRef]
34. Strauss, A.; Corbin, J. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*; Sage Publications: London, UK, 1998.
35. Burgess-Allen, J.; Owen-Smith, V. Using Mind Mapping Techniques for Rapid Qualitative Data Analysis in Public Participation Processes. *Health Expect.* **2010**, *13*, 406–415. [CrossRef] [PubMed]
36. Patton, M.Q. *Qualitative Evaluation and Research Methods*; Sage Publications: Newbury Park, CA, USA, 1990.
37. Calori, R.; Johnson, G.; Sarnin, P. Ceos' Cognitive Maps and the Scope of the Organization. *Strateg. Manag. J.* **1994**, *15*, 437–457. [CrossRef]
38. Eden, C. Analyzing Cognitive Maps to Help Structure Issues or Problems. *Eur. J. Oper. Res.* **2004**, *159*, 673–686. [CrossRef]
39. Sullivan, J.; Lucas, R. *5G Cyber Security: A Risk-Maagement Approach*; Royal United Services Instutute (RUSI): London, UK, 2020.
40. Ruma, L. Cybersecurity in 2020: The Rise of the CISO. *MIT Technology Review*. 24 February 2020, pp. 1–24. Available online: https://www.technologyreview.com/s/615092/cybersecurity-in-2020-the-rise-of-the-ciso/ (accessed on 28 February 2020).
41. Davis, A. Building Cyber-Resilience into Supply Chains. *Technol. Innov. Manag. Rev.* **2015**, *5*, 19–27. [CrossRef]
42. Graca, S.S.; Barry, J.M.; Doney, P.M. Performance Outcomes of Behavioural Attributes in Buyer-Supplier Relationships. *J. Bus. Ind. Mark.* **2015**, *30*, 805–816. [CrossRef]