applied sciences

MDPI

Article

Collaboration Practices for the Cybersecurity of Supply Chains to Critical Infrastructure

Tania Wallis [1,*] and Paul Dorey [2]

[1] School of Computing Science, University of Glasgow, Glasgow G12 8RZ, UK
[2] Information Security Group, School of Engineering, Physical & Mathematical Sciences, Royal Holloway, University of London, Egham TW20 0EX, UK; paul.dorey@rhul.ac.uk
* Correspondence: tania.wallis@glasgow.ac.uk

Abstract: This work describes the collaboration practices of a community of interest in the UK that brings together cybersecurity professionals with a shared interest in improving supply chain cybersecurity for Operational Technology (OT) environments. This research emphasizes the need for collective responsibility between organizations and provides a set of principles for adopting a code of practice and partnership approach to supply chain cybersecurity. This work has enabled cybersecurity experience from several critical infrastructure sectors, including energy, rail, aviation, water, health, and food, to analyze the uptake and practical use of existing supply chain guidance, identifying gaps and challenges. The community has examined touch points with the supply chain and identified improvements related to the communication of cybersecurity requirements, technical and commercial engagement between customers and suppliers, and in the tailoring of implementations towards operational technology contexts. Communicating the context of securing cyber-physical systems is an essential perspective for this community. This work exemplifies a partnership framework and is translating experiences into useful guidance, particularly for OT systems, to improve cybersecurity levels across multiple contributors to critical infrastructure systems.

Keywords: cybersecurity; resilience; supply chain management; operational technology; cyber-physical systems; critical infrastructure; information sharing; systems engineering

check for updates

Citation: Wallis, T.; Dorey, P. Collaboration Practices for the Cybersecurity of Supply Chains to Critical Infrastructure. *Appl. Sci.* **2024**, *14*, 5805. https://doi.org/10.3390/app14135805

Academic Editors: Giorgia Casella, Mirco Peron, Letizia Tebaldi and Eleonora Bottani

Received: 29 April 2024
Revised: 23 June 2024
Accepted: 25 June 2024
Published: 3 July 2024

1. Introduction

In recent years, cybersecurity events impacting Critical National Infrastructure (CNI) have been increasing in quantity and importance [1–3]. The use of the supply chain as an attack vector has increased significantly, with incidents having a knock-on effect on many organizations via their trusted supplier networks. Such events have highlighted the importance of collaborative approaches and a more coordinated and consistent preparation and response to cybersecurity. This is a global issue due to dependencies on international supply chains and similar equipment being used in critical infrastructure in many countries.

Cybersecurity is a shared problem, and it requires shared understanding and partnership to address it. However, policy interventions and resulting regulations can only focus on the cybersecurity obligations of individual organizations. End-to-end security for the technical solutions and services that encompass multiple actors requires interorganizational responses. The effective transfer of risk management responsibilities between organizations and the dividing up of responsibility and accountability is a challenge because the risks are shared in a technically interdependent solution operating across organizationally independent governance structures.

In an attempt to address this, regulations have placed expectations on operators of CNI to take responsibility for the cybersecurity of their supply chains where there is potential impact on the essential services that they provide to society. The cybersecurity assurance of third parties has therefore become more important both during procurement and throughout the lifecycle of a product or service. Due to the scale of dependency on the supply chain, managing these assurance processes as individual organizations involves significant overhead for both customers and suppliers unless a more consistent and shared approach can be adopted. Furthermore, a concentration of risk and dependencies in the supply chain, where there is over-reliance on a few specialized suppliers, is leading to regulators considering regulations also being placed directly on important entities in the supply chain [4,5].

The end-to-end oversight of supply chains for critical infrastructure therefore requires a governance approach where a collective response to cybersecurity can be prepared, uplifting security practices where needed most. This work has defined and built a Supply Chain Expert Group (SCEG) [6], a community of several organizations and individual experts, which recognizes the need to collectively achieve cybersecurity objectives that cannot be addressed by a single organization. This community provides an example of collaborative governance through the willingness of cybersecurity professionals to work across organizational boundaries to protect critical infrastructures more effectively. Its work focuses on the CNI sectors using Operational Technology (OT), including energy, transport, water, health, and food sectors. This enables the pooling of knowledge and gathering experiences from the group to translate into useable guidance consistent across supply chains. It also looks at the creation of practical and simplified guidance to assist companies with fewer resources for cybersecurity. Bringing together cross-sector input to these issues and cross-pollinating experience from other sectors is also assisting progress by stimulating new ideas and solutions. This collaboration is providing a bridge between the UK National Cyber Security Centre (NCSC), private sector companies, and lead Government departments to improve cyber resilience and ensure the policy and regulatory stance is applicable to the technical solutions that form our critical infrastructures. These issues are globally relevant and are also receiving attention from US Government and European Commission initiatives.

2. Related Work

This section considers related research from two perspectives: firstly, guidance is assessed on supply chain cybersecurity coming from governments as well as recommendations and frameworks coming from academic research, including where research is guiding compliance activities for individual organizations. Secondly, research is reviewed that points to the collective and interdependent nature of the supply chain cybersecurity problem and implies the need for partnership approaches to address the interdependencies.

2.1. Guidance on Supply Chain Cybersecurity

The National Institute of Standards and Technology (NIST) provides guidance on supply chain risk management practices [7] that points to ‘agreement documents’ as a vehicle for deciding accountability and responsibility between different service providers and security requirements being detailed in contracts. Working directly with external providers to identify appropriate mitigations is also suggested as a potentially more cost-effective approach [7].

Entities regulated under the NIS directive are obliged to take ‘appropriate and proportionate’ measures to manage cybersecurity risks to their operations and service provision and to prevent or minimize the impact of incidents. This includes addressing risks coming from the supply chain and an entity’s relationship with its suppliers [4].

The European Agency for Cybersecurity (ENISA) [8] expects organizations to define rules for their suppliers and requirements for products and services to protect their information and assets by managing this through contractual arrangements. ENISA recommends supplier relationships be managed with defined rules and processes, including rules for subcontracting to cascade requirements along the supply chain. ENISA also provides good practices for suppliers, integrators, and service providers that are linked to relevant standards [8].

The NCSC has created a set of guiding principles and advises creating a tiered set of supplier security profiles related to the level of potential impact of a supply chain cyber incident to the customer's business and operations. For each security profile, minimum security requirements should be defined and additional requirements provided for higher impact profiles [9]. The NCSC also recommends mapping supply chain dependencies to better understand the cyber maturity of suppliers and focus improvements that are proportionate to the risk [10].

For the energy sector, Oesterreichs Energie [11] defines security requirements for technical components and systems for both the procurement and implementation phases of control systems. It also recommends maintenance processes to be agreed with suppliers and defined in contracts [11].

Boyes [12] provides a model for cyber-physical systems that augments Parker's framework for information security [13] with facets of trustworthiness. This model is applied to the supply chain from three perspectives: continuity of operations, control of access and system operations, and integrity utility and authenticity of information including the system's configuration [12].

Bomhard and Daum [14] review the growing challenges of including cybersecurity in contracts, recommending customized contract annexes to provide customer specifics within standard service contracts. The cybersecurity requirements specified in contracts can become set at the conclusion of the contracting process unless they can encompass future threats that are constantly changing. It is suggested to 'dynamically refer' to the latest guidance and recommendations that are regularly published and updated [14].

Cinar [15] provides a practical contribution with strategies to help manage risks in the supply chain including a five-step process for companies to identify, prioritize, and mitigate supply chain risks [15].

2.2. Partnership in Supply Chain Cybersecurity

Different aspects of collective cybersecurity activity have been described by the literature as follows.

Parker et al. [16] emphasize the importance of engaging vendors in cybersecurity considerations throughout, including during design, build, and implementation as well as in the ongoing evolution of cybersecurity in a changing threat landscape [16].

The 'extreme interconnectedness' and 'urgent problem' of cybersecurity across supply chains are introduced by Melnyk [17], who raises the need for combining observations from different actors and for alignment of supply chain organizations behind a common objective. Melnyk questions if the focal firm can individually fulfill the role of 'change agent' in this space and suggests this might be better achieved by a consortium of companies, academia, and government [17].

Borchert [18] recommends stakeholders co-produce information together, moving beyond information sharing between organizations to shared ownership of information. This would aim to provide actionable information for tackling immediate threats and improve understanding of the broader context of unfolding developments and future risks. The need to organize information flows between stakeholders necessitates a process-based approach, to improve preparations and continuously adapt to a changing security environment [18].

Shaked et al. [19] emphasize a whole systems approach to guide progress in cybersecurity maturity levels. This work identifies 'domains of practice' and 'dimensions of operation' as a means to evaluate cyber maturity by highlighting characteristics that contribute to the emergent properties of the sector, as its constituents interact [19].

Gupta [20] examines the interlacing of physical and virtual supply chains through case studies in additive manufacturing. Gupta recommends a collaborative approach involving engineering and design teams with security in developing defense methods [20] due to the potential for attacks to impact physical equipment within cyber-physical systems.

A survey of the cybersecurity challenges of the supply chain in a defense and military context [21] proposes the need for semantic modeling to discover technology intersections and interdependencies and a synergy of business processes for a 'mutually beneficial environment'. Sobb et al. identified that research is needed on 'what the risks truly are in an operational context' and to understand what factors would inform how integrated technologies 'affect the cybersecurity of their respective systems' [21].

Meagher provides a useful worked example to guide compliance activities for an organization [22]. This work designed a 'Cyber INTEL' framework for aligning cyber-resilience activities with cybersecurity regulations and standards. This framework is applied to a fictional manufacturing company to demonstrate achieving compliance with relevant cyber laws, such as NIS2 [4], GDPR [23], and the NIST Cybersecurity Framework [24]. This worked example briefly mentions third-party responsibilities in relation to a wide area network that links three manufacturing plants and recommends vetting alternative suppliers of critical materials in business continuity planning. The gaps identified by Meagher's analysis include a missing layer of governance for supply chain risks and managing third-party vendors. This was highlighted as a 'high-risk impact' requiring 'immediate attention' [22].

2.3. Research Aims and Contribution

The above related works [7,8,11], on the whole, treat products and services as items to be secured separately from the customer organization and recommend this to be managed through requirement definitions and contractual arrangements.

The novelty and originality in our work is the focus on assurance of products/services within the customer environment, where suppliers are contributing to the resilient operation of the purchasing customer. This requires partnership and integrated processes with suppliers, where responsibilities cannot easily be divided and a collective responsibility emerges. Our work provides a framework for working more directly with external providers to mitigate risks, as suggested in [7].

When activities are outsourced to suppliers, the overall risk ownership remains with the purchasing customer, and suppliers are contributing to the operational risk that is owned by the customer. This calls for effective interworking between customer and supplier organizations. This research provides a foundation for collaboration practices that aims to support a more effective contribution from suppliers to the cybersecurity of their customers' solutions.

The authors' previous collaborative work with the UK energy sector [25] has shown that NCSC principles can be used as the basis for the creation of more specific guidance to assist energy companies with a common, whole sector approach to supply chain cybersecurity. In that work, risks were related to the product or service being provided, and security requirements were specified for each type of supplier, such as service operators, maintainers, manufacturers, and systems integrators. Also, that work introduced supply chain cybersecurity as a shared problem and proposed a partnership approach with dialogue between customers and suppliers, introducing the concept of a code of practice that is founded in partnership for effective cybersecurity *with* the supply chain [25].

In Section 2, this paper describes how the SCEG was established. A reference model is provided in Section 4.1 that has enabled an analysis of interaction points with the supply chain. Outputs produced during the first year of the SCEG collaboration are outlined in Section 4.2, Section 4.3, Section 4.4. These outputs emerged from the interests of the group and from topics that were relevant to their industry roles. These outputs are therefore limited by the experience and sectors represented in the SCEG. Initial outputs are assisting companies with standards and assurance. Later outputs navigate towards partnership thinking, such as preparing and responding to incidents with suppliers involved.

The work also explored perspectives from different CNI sectors on our previously proposed Code of Practice and Partnership (CoPP) approach [25] and has applied and further developed these partnership principles by defining partnership practice statements in Section 4.5. Section 5 discusses the findings, and Section 6 concludes the contribution of this research and introduces planned future work. Table 1 shows the structure of this research.

Table 1. Structure of the research.

Research Design	
Objective	To propose and exercise a partnership approach to supply chain cybersecurity. Provide a practice framework as a foundation for collective responsibility between organizations.
Literature Review	A review of the literature that recommends cascading cybersecurity requirements along the supply chain with contracts and agreements that separate responsibilities. An overview of research that highlights the lack of governance for supply chain risks and the interdependencies involved and calls for a consortia of companies, common approaches, and combined observations to address the problem.
Proposed Approach	A code of practice and partnership approach to guiding supplier contributions to the cybersecurity of CNI.
Case Study	The design and build of a supply chain expert group to exercise partnership working.
Recommendations	A supplier engagement reference model to guide interaction points with suppliers and increase information flow between partners. Practice statements are provided to set a partnership foundation between interdependent organizations.
Future Work	Research the practice of applying new NCSC supply chain guidance to OT environments to propose how this can work in practice. Design an illustrative responsibility model with generic templates to guide the combined responsibilities of customer, suppliers, and regulator.

3. Materials and Methods

This research includes transdisciplinary characteristics [26] by focusing on the real-world problem of supply chain cybersecurity and involving non-academic participants in the process. By working with a transformative approach, this research has proactively supported industry and government actors and by continually reflecting on broader contexts is providing impact beyond academic outputs. This research has an applied orientation to contribute towards improving practices and required both academic and non-academic actors to engage in a process of co-creating new knowledge.

A practice space was created by convening a group of potential collaborators with a shared interest in supply chain cybersecurity. Initially, a review of the skill sets, knowledge, and experience of the members built an understanding of the expertise in the group. Introducing an overview of the problem area set the common ground for the collaboration. By developing and communicating a shared vision, the group could proceed with an integrative approach to combine skill sets through a process of sharing and analysis to form a synthesis of experiences and practices. Where possible, this was then translated into usable guidance to enable cybersecurity improvements suitable for an OT context. The essential components to establishing such a collaborative practice space are detailed in Table 2.

This resulted in an OT cybersecurity Supply Chain Expert Group (SCEG) involving 40 active members across operators, suppliers, consultants, academia, and NCSC to exercise partnership approaches involving several sectors and to define partnership practices. Attracting Operational Technology (OT) experience to the group was essential to form an OT context as a backdrop to all the work items, ensuring recommendations were suitably specific for OT deployments, and to improve understanding of the context of OT among relevant stakeholders. The support of the NCSC, the respected UK technical authority, has provided credibility to attract high-caliber participants, but notably the NCSC has encouraged the group to generate its own thinking and firmly ground the work in the needs and experiences of the private sector operating CNI.

Table 2. Components of a collaborative practice space.

Founding a Collaborative Practice Space
Define the reason for the practice space, introducing the challenge and the problem to be addressed.
Convene the group—inviting different perspectives on the issue to enrich the work with multiple perspectives.
Set the common ground for the collaboration—with rules of engagement.
Develop and communicate a shared vision together, defining the context for the practice.
Know the group—meet them where they are—get to know the knowledge, experience, and expertise in the group. To meet them where they are at and invite contributions, with the goal in mind and the objective communicated.
The synthesis—a process of sharing and analysis to form a synthesis of experiences and practices, broadening perspectives, addressing gaps, together constructing new knowledge.
Creative effort, co-producing outputs—content provided from different experts is reviewed by all and discussed in meetings to develop further insights together. Translation of the work into actionable guidance is encouraged to enable cybersecurity improvements suitable for an OT context to be shared beyond the practice group.
To establish a creative and committed group, members are involved in the direction and ownership of activities to foster motivation to contribute and address topics that were relevant and useful to members. The group defines their own priorities and outputs, and the group is facilitated and supported (not 'managed' or directed) by the group's coordinators.

The SCEG placed importance on listening to the perspectives of different participants, OT and safety, cyber and physical security with the aim to co-produce improved guidance and best practices. The SCEG enabled a two-way exchange, exploring both sides of the customer and supplier story. The group has supported the process of customer security expectations being placed on suppliers and is also balancing this with an emphasis on the supplier perspective. From the early stages, the group therefore looked from the other direction, from the supplier toward the customer, to also give a voice to supplier experiences in the process. Suppliers are often lacking information in terms of what security capability they need to deliver, including addressing potential gaps in customer capability and how their component could influence the overall risk picture in a customer's operation. Content and discussion were opened up to wider review beyond the group on a regular basis to improve outcomes and reach of the work.

The group is different to an Information Sharing and Analysis Center (ISAC) that is typically for a specific sector. Many suppliers provide products and services to several sectors, so it was appropriate to form a group involving different sectors. An unexpected benefit was revealed in feedback from the group that they found it very useful to meet and discuss with other sectors. For example, progress viewed in one sector was inspiring other sectors to see a path to improvements. ISACs are also almost entirely focused on operational and tactical information sharing rather than strategic change as required in examining how organizations will operate together and determine future responsibilities.

The SCEG has used its prior experience to build a group culture to leverage initiatives, encouraging and energizing contribution to create tangible results, establishing a supportive environment as a foundation for activities to be performed consistently and effectively. Rather than leading the SCEG like a project that imposes external targets and deadlines on members, it was important for the success of this volunteer work group for members to be included in the direction and ownership of activities to foster motivation to contribute and address topics that were relevant and useful to members. It took time to set these foundations and establish a creative and committed group.

After an initial period of building relationships through knowledge sharing, the structure of the work program was then created. An on-line repository was provided for sharing and working together. Discussion meetings captured a gap analysis, which resulted in ten work items for the group to co-produce. A lead member, based on their own expressions of interest, was identified for each work item, and individual members agreed to create content for or review each of the topics. Outputs are made specific to ICS and OT cybersecurity and provide industry-based illustrations of best practice and case studies of NCSC principles. The work items aim to be detailed enough to guide the implementation of OT cybersecurity improvements across CNI supply chains without the need for a customer or supplier to have dedicated teams of professionals to provide an interpretation. To provide an overall context for the different parts of guidance, an analysis of the supplier engagement process was carried out by the group to create a common reference model. This is being used to bring together the different SCEG outputs into a process flow. Initial outputs of the group produced during its first year are described in Section 3.

4. Results

This section describes the reference model that was developed by examining the stages of interaction with the supply chain during the lifecycle of a product or service. This section also describes the initial SCEG outputs and provides practice statements to define the partnership principles.

4.1. Supplier Engagement Model

To enable the interactions between customers and suppliers to be better understood and analyzed, the collaborative workgroup developed and agreed upon a generic model for customer/supplier touchpoints in a supply chain. This ran from procurement through the life of a product or service and even considered close-out. This was used to identify where there was effective transfer of risk management responsibilities or knowledge relating to cybersecurity. It also identified examples where there have been benefits from a mutual commitment to cybersecurity with proactive and useful information flows between partners. The model was also used to highlight gaps and challenges in common practices, which are described later in this paper.

Figure 1 shows the generic supplier engagement process flow and the touchpoints with the supply chain. The most common artifacts or techniques used at particular stages (e.g., a Request For Information questionnaire—RFI) were also identified for each stage.

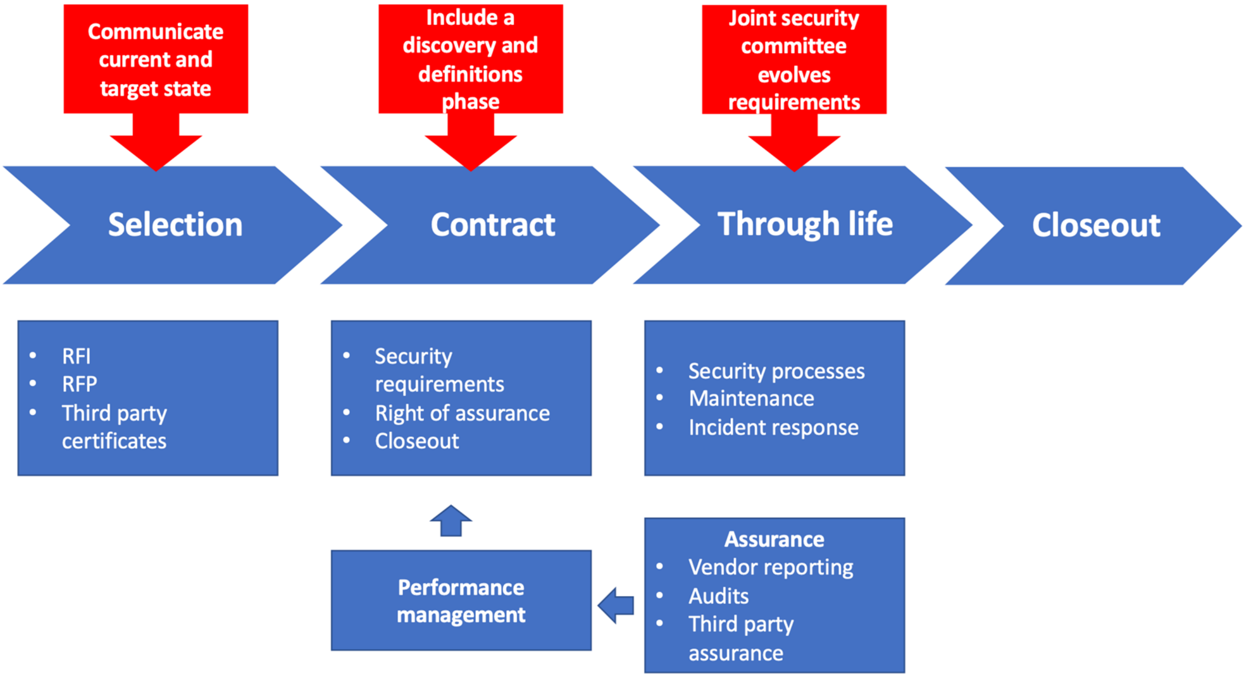


Figure 1. Generic supply chain interaction process flow, including common techniques and artifacts used at each stage.

The SCEG defined the different stages in the process, identified the key tools and sub-processes, and then shared their experience on how well these worked in practice, particularly highlighting any gaps. Table 3 highlights the key findings from examining this supplier engagement reference model and the following sub-sections present each stage with the views of the experts.

Table 3. Key findings from supplier engagement reference model.

Selection	Contract	Discovery	Through Life	Closeout
Provide motivation to propose secure solutions within tendering rules.	Assist synergy between commercial and technical requirements.	Communicate operational risks to help vendors propose secure solutions.	Integration of security processes in the customer environment.	Exit plan agreed upfront, regain control of assets, close access to info and systems, how data will be deleted.
Communicate security status of current systems and target security objectives.	Create specific contract wordings for OT network infrastructure and OT InfoSec policy.	Clear definition of cybersecurity requirements for delivery.	Address changes in threat, risk, regulations.	Manage knowledge transfer.
		Define roles and responsibilities.	Exercises to test how you work together to manage incidents.	Retain contacts for future incidents.

4.1.1. Selection

Selection generally follows a process where the supplier organization is shortlisted via a Request for Information (RFI) and then their product or service is matched to the more detailed requirements of the customer—often through a request for proposal (RFP) to help decide to procure or reject a particular proposal.

In the opinion of the experts in the workgroup with experience in multiple sectors, it was much more common for organizations to just issue an RFI in the context of cybersecurity and thus select that capability at a supplier corporate level. Going on to focus cybersecurity assessment in the detail of an RFP with specific risks in mind is therefore seen as a sign of greater maturity in a customer's third-party risk management processes.

The experts also stated that they saw that the lack of specific detail in defining cybersecurity requirements even occurred within RFP processes, where it was rare in the tendering process that the customer would provide a detailed security status of current systems and their target security objectives. Several experts went on to provide illustrations where procurement processes without well-defined cybersecurity may run afoul of procurement rules where a supplier is not permitted to raise matters considered to be out of scope. This can prevent suppliers from proposing secure solutions or flagging identified security concerns and can therefore prevent relevant and appropriate security from being included in product and service offerings.

The experts noted that going into more detail on security requirements does run the risk of increasing complexity and workload for both customers and suppliers due to having to create and respond to bespoke security control frameworks and checklists. It was therefore seen to be important to reference common standards. Representatives from suppliers in particular stressed the importance of using international standards to reduce unnecessary regional customization.

The unwelcome overhead of having multiple RFI questionnaires/processes and diverse RFP topics [12] along with the energy sector solutions of creating a standardized RFI and common RFP guidance are described in [25]. The cross-sector expert group gave this further consideration and identified the challenge of declaring a common standard set that could work across multiple sectors—particularly important for suppliers serving several sectors with common products and services. The group therefore set itself the task of seeing if a workable standards set could be declared for OT systems (considered more diverse than office IT systems) across multiple CNI sectors.

The expert group also identified the value of using pre-existing company certifications, such as ISO 27001 [27] and the UK Cyber Essentials [28], the advantage here being reuseability with customers and suppliers not having to re-perform work for each new engagement. However, it was noted that lack of understanding of the scope of a certification could be misleading and could result in a certificate that does not cover the actual product or service being procured. An illustration of this is that the common examples of certifications currently used in procurement cover IT and not OT environments. The group therefore set itself the task of choosing a well-established attestation process and seeing if it could be easily adjusted and applied to the scope and context of OT systems, as described in Section 4.3.

The results of the analysis of the selection phase and the resulting actions relevant to OT and the expert group are summarized in Table 4.

Table 4. OT actions arising in selection phase.

Activity/ Tool	Purpose	Issue Identified	Results and Actions
RFI	Selection of a supplier with good cybersecurity practices.	Multiple questionnaires and duplicated processes.	UK Energy sector has produced a common RFI. More work is needed on how to promote adoption.
RFP	To define cybersecurity requirements for the specific product or service.	Diverse number of requirements, insufficient detail.	UK Energy Sector has produced guidance on RFP key topics. More guidance is needed on how to define current and target state.
Standards Referenced	To simplify defining security requirements and solutions.	Unclear which standards to choose from a very long list.	Simplified guidance (in Section 4.2) has been produced to declare key standards, particularly cross-sector and internationally accepted. More detailed guidance for individual sectors will be provided in future work.
Certification	To provide pre-worked assurance of cybersecurity status.	Lack of cybersecurity service certification for OT systems.	Currently testing to see if a common attestation scheme can be adjusted to address OT. Also, the SCEG is currently creating a framework for categorizing assurance tools.

4.1.2. Contracts

It became apparent, due to the differences between IT and OT, that OT needs have not been addressed well in contractual arrangements. Because of the different risk profiles, specific contracts/sets of requirements are required for network infrastructure interacting with OT along with OT-specific security policies.

Contractual clauses can be used for the transfer of risk management responsibilities to suppliers, but such commitments are potentially ineffective in actual implementation if not supported by an exchange of technical information and clarifications relevant to the service provision. High-level contract clauses do not provide the necessary level of detail that ensures implementation at the required security level. The expert group suggested that a discovery and definitions phase could aid this process and assist more synergy between commercial and technical requirements. However, contracts are tools used to focus on unambiguous responsibilities and assign liability rather than encourage collaboration. If cybersecurity is inadequately specified to suppliers, then all aspects of managing the risk remain fully with the customer.

The delivery of the management of risk could be more effective as a conversation and a process. It was proposed that a collaborative discovery process of emerging security risks should be facilitated. The actual definition of cybersecurity requirements for delivery requires a risk assessment to indicate security levels with different resulting requirements. Communicating operational risks, describing threats, and capturing risk tolerance would help suppliers to propose appropriately secure solutions. However, discussing and refining requirements is heavy on customer and supplier resources and increases the overhead of contract negotiation. Therefore, having defined standard requirements for different security levels would be helpful.

4.1.3. Through Life and Assurance

Due to the changing nature of cybersecurity, the group recommended extending supplier assurance activities throughout the contract lifecycle to define what the ongoing support will be for integrating and maintaining security in the customer environment. The roles and responsibilities for assurance also need to be clear. Where contracted services are complex and likely to change, the group has proposed that ideally a joint security committee of supplier and customer representatives should address ongoing changes in threats, risks, and regulations and be able to evolve and re-specify security requirements as necessary. Such a committee could also be engaged to establish processes and relationships between company 'first responders' to enable the management of incidents across customer and supplier companies and promote the testing of processes through collaborative exercises. Cyber-attacks can also take advantage of any weaknesses or false assumptions in the trust relationship between customer and supplier. Defining the specifics of their trusted engagement would help avoid exploiting inherent trust by the customer in their supplier. Inherent in running OT is also the need to establish support for critical ongoing operations; this raises the importance of maintaining supplier relationships for managing risks throughout the lifecycle. There is a risk that the through-life operational cost of cybersecurity may not be fully considered unless the scoring criteria during procurement recognize both initial investment and ongoing operational expenditures. Budgets need to be realistic through life and need to address change in threat, risk, and regulatory expectations. Security can be dynamic in its demands during the life of a contract, and this makes costing a challenge.

4.1.4. Closeout

The group pointed out that the closure stages of a contract relationship must also be considered in advance, emphasizing the importance of having an exit plan agreed upfront, for example, to regain control of assets, close access to information and systems, and agree how data will be deleted. Managing knowledge transfer before closeout and maintaining contacts in case of future incidents are also important.

4.2. Declaring Standards

As mentioned in Section 2, a dive into standards and regulations is provided with a worked example by Meagher [22]. ENISA also provide guidance that is linked to relevant standards [8]. This section describes the work of the SCEG to provide a review of the most utilized standards in supply chain cybersecurity.

Practice experience was gathered from the SCEG members and representatives for each CNI sector on the most important and relevant standards being used in supply chain cybersecurity assurance for OT. This has been collated and presented as an infographic and is intended to give companies a head start in navigating available standards. Due to significant skill shortages in cybersecurity and the different perspective of OT deployments, it is really important and necessary to find ways to disseminate knowledge such as this assistance with navigating standards. The group also considered that it was important to highlight where any well-accepted standards did or did not require payment of a license fee as cost was seen to be an inhibitor for smaller organizations.

There are further layers of detail planned for this work to elaborate on the information shown in the infographic. This first stage release is shown in Figure 2, and additional layers with more detailed practice experience of utilizing standards per sector will be provided in future work.

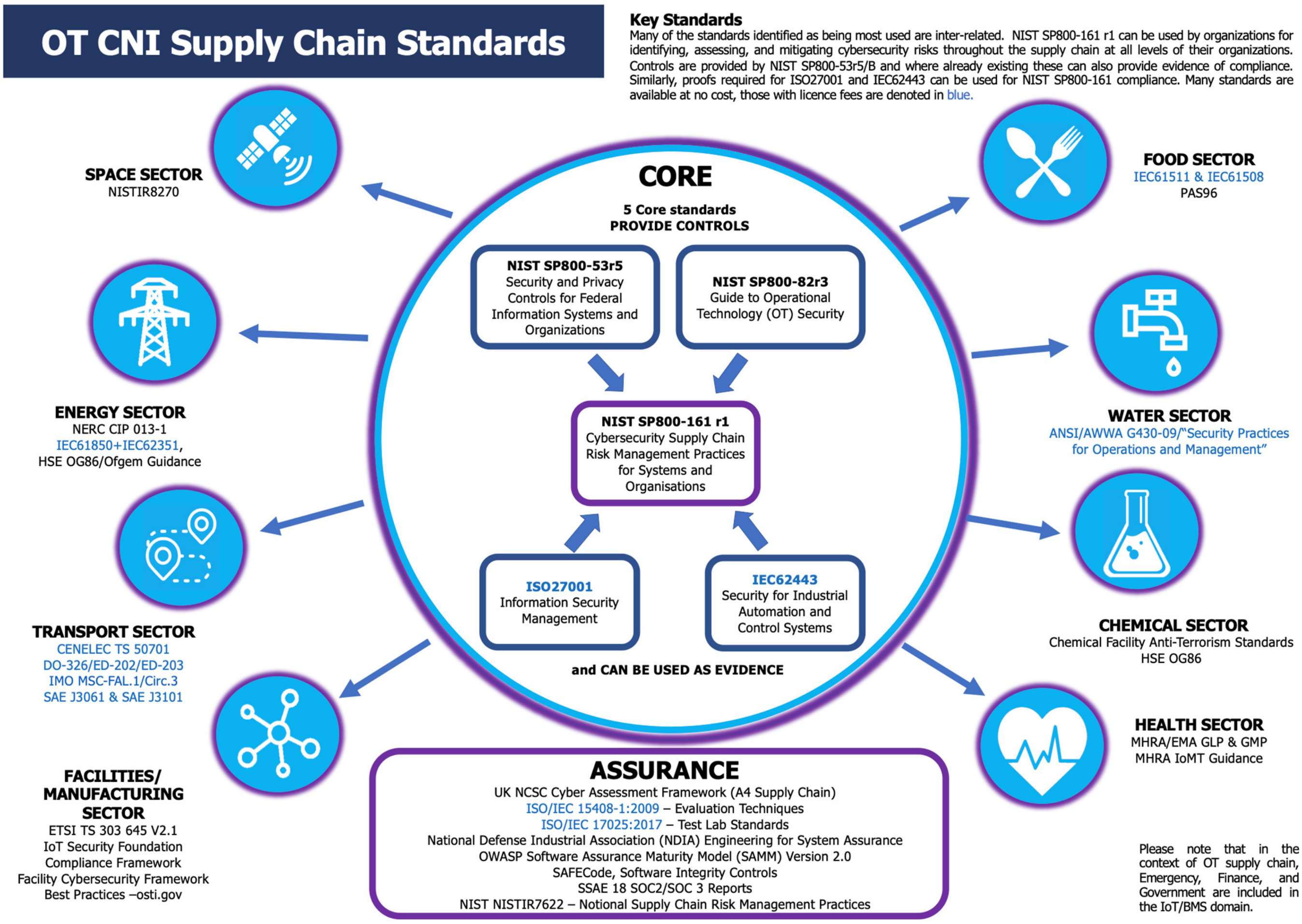

OT CNI Supply Chain Standards
Key Standards
Many of the standards identified as being most used are inter-related. NIST SP800-161 r1 can be used by organizations for identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations. Controls are provided by NIST SP800-53r5/B and where already existing these can also provide evidence of compliance. Similarly, proofs required for ISO27001 and IEC62443 can be used for NIST SP800-161 compliance. Many standards are available at no cost, those with licence fees are denoted in blue.
CORE
5 Core standards
PROVIDE CONTROLS
NIST SP800-53r5
Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP800-82r3
Guide to Operational Technology (OT) Security
NIST SP800-161 r1
Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations
ISO27001
Information Security Management
IEC62443
Security for Industrial Automation and Control Systems
and CAN BE USED AS EVIDENCE
SPACE SECTOR
NISTIR8270
ENERGY SECTOR
NERC CIP 013-1
IEC61850+IEC62351,
HSE OG86/Ofgem Guidance
TRANSPORT SECTOR
CENELEC TS 50701
DO-326/ED-202/ED-203
IMO MSC-FAL.1/Circ.3
SAE J3061 & SAE J3101
FACILITIES/ MANUFACTURING SECTOR
ETSI TS 303 645 V2.1
IoT Security Foundation Compliance Framework
Facility Cybersecurity Framework
Best Practices –osti.gov
FOOD SECTOR
IEC61511 & IEC61508
PAS96
WATER SECTOR
ANSI/AWWA G430-09/"Security Practices for Operations and Management"
CHEMICAL SECTOR
Chemical Facility Anti-Terrorism Standards
HSE OG86
HEALTH SECTOR
MHRA/EMA GLP & GMP
MHRA IoMT Guidance
ASSURANCE
UK NCSC Cyber Assessment Framework (A4 Supply Chain)
ISO/IEC 15408-1:2009 – Evaluation Techniques
ISO/IEC 17025:2017 – Test Lab Standards
National Defense Industrial Association (NDIA) Engineering for System Assurance
OWASP Software Assurance Maturity Model (SAMM) Version 2.0
SAFECode, Software Integrity Controls
SSAE 18 SOC2/SOC 3 Reports
NIST NISTIR7622 – Notional Supply Chain Risk Management Practices
Please note that in the context of OT supply chain, Emergency, Finance, and Government are included in the IoT/BMS domain.

Figure 2. OT CNI supply chain standards [1,3,4].

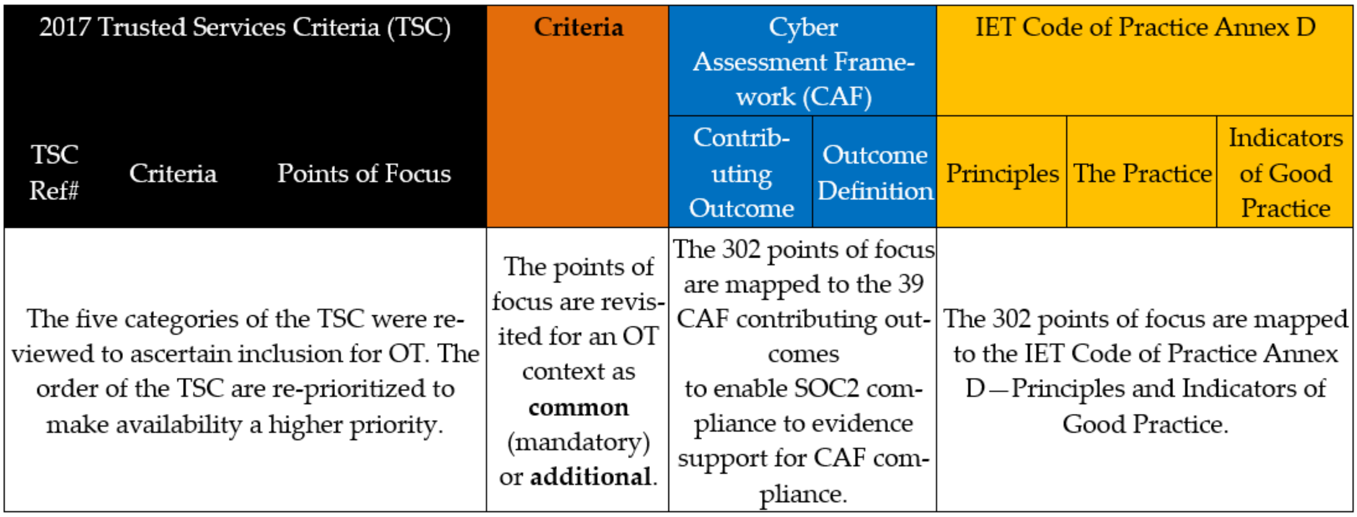
4.3. Validating OT Security through a Trusted Third Party—Translation to OT Context

Supplier assurance improves understanding of the cybersecurity risk management status between companies and ensures that a supplier, technology, or service that a customer business relies upon has an acceptable level of cybersecurity maturity. Assurance enables businesses to make risk mitigation decisions based on the degree of evidence of compliance and subsequent trust. Use of an independent assurance provider can also provide in-depth evidence and verification and confirm ongoing compliance with contracts and regulations. The advantage of using a third party is the reduction of effort by the customer, and it may reduce work by the supplier if the same assessment can be re-used by other customers.

A review of commercial assurance service provider provisions and how well they address OT has been carried out within the SCEG by members sharing their experience of the market. This review discovered a focus on IT and financial assurance and found very limited third-party assurance provision that directly addresses OT cyber risks. To test the potential extension of established IT assurance processes to cover OT, it was decided to review the SOC2 trusted service criteria. SOC2 is a well-established auditing procedure under the International Federation of Accountants [29] to assure the security of service providers. The trusted service criteria include: security, availability, confidentiality, processing integrity, and privacy. These were reviewed from the perspective of OT and re-prioritized towards OT needs, such as availability being prioritized above privacy.

In addition, these criteria and points of focus have been mapped to the Cyber Assessment Framework (CAF) [30] provided by NCSC, to align the work with a framework familiar to industry end users and to assist them with identifying key areas for assessment and to decide the scope of assurance and use the findings to target on-site audits. Due to the importance of including safety considerations in assessments, an additional mapping was carried out according to Annex D of the Code of Practice for Cybersecurity and Safety [31] that provides indicators of good practice for the assurance of safety and security. This SCEG output is an example of existing guidance needing translation and extension to be applicable to an Operational Technology (OT) environment.

Figure 3 below provides a snapshot of this work, and a detailed version of this output is available on the SCEG's web presence [6].



2017 Trusted Services Criteria (TSC)			Criteria	Cyber Assessment Framework (CAF)		IET Code of Practice Annex D		
TSC Ref#	Criteria	Points of Focus		Contributing Outcome	Outcome Definition	Principles	The Practice	Indicators of Good Practice
The five categories of the TSC were reviewed to ascertain inclusion for OT. The order of the TSC are re-prioritized to make availability a higher priority.			The points of focus are revisited for an OT context as **common** (mandatory) or **additional**.	The 302 points of focus are mapped to the 39 CAF contributing outcomes to enable SOC2 compliance to evidence support for CAF compliance.		The 302 points of focus are mapped to the IET Code of Practice Annex D—Principles and Indicators of Good Practice.		

Figure 3. Re-prioritizing for OT and mapping to CAF.

4.4. Addressing Incident Response with the Supply Chain

The SCEG provided input to the guidance for industry on developing incident response and management *with* the supply chain. This work has also been enhanced with input from beyond the SCEG membership to also include cross-sector incident response experience from thirty individuals/organizations. This is a living document that will be updated with new experience over time and is available on the SCEG website [6].

This work in particular stressed the importance of developing a mature understanding of vendor deployments in IT and OT to assist with understanding the impact and potential extent of exploits and to be able to focus resources on impacted systems.

Some of the key points covered are provided in Table 5.

Table 5. Developing incident response and management with the supply chain.

Incident Response with the Supply Chain
Incident response as a team effort with business stakeholders.
Supplier engagement in both preparation and response to incidents.
Embed cybersecurity awareness with suppliers and departments, e.g., procurement and legal.
Maintain understanding of the risk associated with providing products/services to a customer organization.
Have supplier risk assessments on record to assist with initial impact assessment.
Develop supplier-specific playbooks with key suppliers.
Carry out joint cyber-related exercises with suppliers.

4.5. Partnership Principles and Practice

Previous work with the energy sector introduced partnership principles [25] that have now been further tested with the Supply Chain Expert Group and other CNI sectors, resulting in twelve practice statements that define the Code of Practice and Partnership (CoPP) approach, as detailed in Table 6. This CoPP approach has been launched with the energy sector in the UK and will form the basis of supplier network collaborations in other sectors in future work.

Table 6. CoPP core principles and practice statements.

Core Principles	Partnership Practice Statements
Basic Security Is Foundational	1. Designed in security Security will be designed into products and services with a design informed by threat and the context of where and how the product and service will be used. Suppliers will provide secure deployment/engagement guides, such as defining secure by a default system delivery.
	2. Security by default Good security practices, including regulatory obligations and secure information handling, will be requested by the customer, established by default by the supplier, and confirmed by agreement. Staff, including third-party systems integrators, will be required to follow the agreed-upon good practices and be expected to be trained in doing so. Good practices may require a collaborative work group to develop or declare from existing standards (e.g., device hardening).
	3. Securely developed Systems will be built and developed in a secure environment by security-trained developers using a robust secure development lifecycle [32]. Additionally, secure engineering will tailor solutions to the context of end use to provide functional resilience and secure operation of the system in the customer environment.
	4. Maintained through life Security will be maintained and kept updated in a timely manner and throughout a 'reasonable' lifetime to goals clearly stated upfront in commercial terms. The stated lifetime will include a migration path for upgrade or risk mitigation where a fourth-party vendor component goes out of security support.
Security Needs Collective Responsibility	5. Combined incident management Suppliers and customers will share knowledge and expertise to work together in the management of incidents and will participate in collaborative exercises to test those processes. The need for separate or combined exercises will depend on the nature of the risk and will need to be agreed upon.
	6. Clear roles and responsibilities Services and/or products will be delivered and adopted with a clear definition of the different security roles, responsibilities, and interdependencies between supplier and customer.
	7. Integrated systems and processes Suppliers and customers will support the integration of security processes and technologies in the customer environment. This will include adopting industry APIs and protocols for security management reporting interfaces. Security management processes, such as for identity and access management or alerting, will be appropriately linked between supplier and customer.
	8. Mutual innovation and support Both suppliers and customers recognize the need to work together (such as developing common guidance, responsibility templates, or reference architectures) in collaborative cybersecurity forums to manage risk, help in meeting regulatory requirements, and also benefit from the opportunities of new technologies and business models. For specific engagements, suppliers and customers may well combine their security expertise.
Transparency and Communication Are Key	9. Risk awareness Both suppliers and customers will inform one another about relevant current or emerging security risks through a collaborative discovery process and be open to receiving challenges to their own assumptions, such as a supplier warning a customer if they see a proposed inappropriate use of systems, customers articulating operational risks to help vendors propose secure solutions, or sharing views on emerging business models and/or technologies with new attack surfaces and threats.
	10. Vulnerability reporting Suppliers and customers will operate processes for transparent reporting and appropriate timely handling of vulnerabilities discovered by themselves or third parties, including the operation of a responsible disclosure process.
	11. Assure end-to-end supply chain Suppliers will assure the cybersecurity of their own supply chain and provide the customer with a suitable maintained bill of materials describing the components and software which are integrated into what they provide—for which the NTIA SBOM work is a key standard reference [33]—including when assurance was last confirmed.
	12. Adopt international standards and certification Suppliers and customers will aim to adopt international standards and promote common assurance approaches, tests, and certification, which will be progressed by collaborative work groups as needed.

5. Discussion

The formation and practice of the OT cybersecurity supply chain expert group has brought together a combination of perspectives on cybersecurity across supply chains to critical infrastructure. The resulting view from the SCEG collaboration is that commonly used supply chain management approaches for cybersecurity risk, particularly for operational technology (OT), are not bringing sufficient clarity on roles and responsibilities and do not support a shared understanding of risk. The agreed partnership practices described in Table 6 indicate the need for collaborative practices, working together, integrated processes, and the use of responsibility templates. From an IT perspective, more efficient ways to manage supply chain cybersecurity issues are required for extensive supply chains. In an OT environment, with critical ongoing operations and potential physical impacts, relationships with suppliers become even more important to foster a collective response to the issues.

The sectoral response to supply chain cybersecurity thus far has been to place regulations on individual customer organizations and to provide supply chain management guidance aimed at the practices of individual organizations. Broadbrush security improvements by regulations and guidance for individual organizations definitely bring benefits through incremental improvements but are insufficient in achieving integrated risk management, which must be informed by the context. Without the context, where a supplier is asked to provide a self-assessment or evidence of cybersecurity maturity, they are evidencing their own cybersecurity practices for their own organization and their own risks and not beyond.

Where suppliers are contributing to the risk of others by their product or service being used in the customer environment, then this risk also needs to be addressed: for example, where suppliers are connected to OT networks, they need to come under the cybersecurity management processes of the customer, and responsibilities can become less clear (e.g., joiners, movers, leavers' processes). Suppliers need to at least be provided with clear security requirements and a security risk profile related to the potential impact on the customer's context. This would guide supplier contribution to OT security with clearer direction on what is required of them.

However, responsibility for the oversight of an integrated operation cannot be outsourced. The operator of an essential service retains ownership of the primary risk, i.e., the cybersecurity risks that can impact the operations/business of the essential services provider, even when aspects of the service are outsourced. This remains a confusing concept in supply chain management, so the SCEG group considers that a clearer model describing responsibilities and interactions would be of value.

6. Conclusions and Future Work

Establishing this expert group has set the foundation to provide a deep dive into OT experiences of applying cybersecurity in this domain. Practice statements have been developed to define the partnership approach to supply chain cybersecurity.

Rather than mitigation of risks in the supply chain through contract management, this group is giving attention to collective responsibility within customer–supplier partnerships and how that can work in practice. This paper provides the initial outputs of the SCEG group and presents the concepts and the foundation that are now in place for further exploration of a CoPP approach per sector in future work. The outputs reflect and synthesize the experience and sectors represented by the 40 members of the SCEG. To address this limitation, wider review and input has been sought to improve the SCEG outputs and continued improvement is invited via the SCEG's web presence [6].

Future work will gather the in-practice experience of applying the latest NCSC supply chain guidance [9,10]. This aims to provide a working example of supply chain cybersecurity in CNI and how it works in practice. Experiences in the SCEG have found that even if the expected process and methods defined in the standards and guidance are followed, additional descriptions at organization interaction points are needed to guide the process to the required level of detail. For example, standards require information to be passed from customer to supplier during the specification and the flow down of security requirements, but there is a lack of detail on how this should happen, such as what information is needed, where responsibilities lie, or deciding the boundaries between responsibilities. Future work will therefore look at the feasibility of creating a generic model to support the definition of customer, supplier, and regulator boundaries and how to define the responsibilities of each group. The aim is to derive an illustrative responsibility model from scenarios drawn from different sectors.

Author Contributions: Conceptualization, T.W. and P.D.; methodology, T.W. and P.D.; validation, T.W. and P.D.; formal analysis T.W. and P.D.; investigation, T.W. and P.D.; resources, T.W. and P.D.; writing T.W. and P.D.; visualization T.W. and P.D.; funding acquisition, T.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by EPSRC Impact Acceleration Account EP/X5257161/1.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: The ongoing support and contribution of the SCEG members are gratefully acknowledged [6].

Conflicts of Interest: The authors declare no conflicts of interest. The funder had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. National Cyber Security Centre. NCSC Warns of Enduring and Significant Threat to UK' s Critical Infrastructure. Available online: https://www.ncsc.gov.uk/pdfs/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure.pdf (accessed on 23 April 2024).
2. ENISA. Threat Landscape for Supply Chain Attacks. Available online: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (accessed on 23 April 2024).
3. Bıçakcı, S.; Evren, A.G. Responding Cyber-Attacks and Managing Cyber Security Crises in Critical Infrastructures: A Sociotechnical Perspective. In *Management and Engineering of Critical Infrastructures*; Academic Press: Cambridge, MA, USA, 2024; pp. 125–151. [CrossRef]
4. European Union. EU DIRECTIVE on Measures for a High Common Level of Cybersecurity across the Union. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 (accessed on 24 April 2024).
5. UK Department for Science Innovation & Technology. Protecting and Enhancing the Security and Resilience of UK Data Infrastructure. Available online: https://assets.publishing.service.gov.uk/media/657ab6f6254aaa000d050ce2/protecting_and_enhancing_the_security_and_resilience_of_UK_data_infrastructure.pdf (accessed on 24 April 2024).
6. Dorey, P.; Wallis, T. Industrial Control Systems Community of Interest Supply Chain Expert Group. Available online: https://ritics.org/ics-coi-sceg/ (accessed on 7 June 2024).
7. Boyens, J.; Smith, A.; Bartol, N.; Winkler, K.; Holbrook, A.; Fallon, M. *Cybersecurity Supply Chain Risk Management for Systems and Organizations*; National Institute of Standards & Technology: Gaithersburg, MD, USA, 2022. [CrossRef]
8. Papaphilippou, M.; Moulinos, K.; Theocharidou, M. Good Practices for Supply Chain Cybersecurity. Available online: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity (accessed on 5 June 2024).
9. National Cyber Security Centre. How to Assess and Gain Confidence in Your Supply Chain Cyber Security. Available online: https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security/stage-2-develop-an-approach/stage-2b-create-key-components-for-your-approach (accessed on 21 April 2024).
10. National Cyber Security Centre. Mapping Your Supply Chain. Available online: https://www.ncsc.gov.uk/guidance/mapping-your-supply-chain (accessed on 21 April 2024).
11. Österreich E-Wirtschaft & Bundesverband der Energie- und Wasserwirtschaft e.V. Whitepaper Requirements for Secure Control and Telecommunication Systems. Available online: https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf (accessed on 5 June 2024).
12. Boyes, H. Cybersecurity and Cyber-Resilient Supply Chains. Technology Innovation Management Review. *Technol. Innov. Manag. Rev.* **2015**, *5*, 28–34. Available online: https://timreview.ca/article/888 (accessed on 2 June 2024). [CrossRef]

13. Parker, D.B. Toward a New Framework for Information Security? In *Computer Security Handbook*; Wiley: Hoboken, NJ, USA, 2012. [CrossRef]
14. Bomhard, D.; Daum, A. Cybersecurity in Outsourcing and Cloud Computing: A Growing Challenge for Contract Drafting. *Int. Cybersecur. Law Rev.* **2021**, *2*, 161–171. [CrossRef]
15. Cinar, B. Supply Chain Cybersecurity: Risks, Challenges, and Strategies for a Globalized World. *J. Eng. Res. Rep.* **2023**, *25*, 196–210. [CrossRef]
16. Parker, S.; Wu, Z.; Christofides, P.D. Cybersecurity in Process Control, Operations, and Supply Chain. *Comput. Chem. Eng.* **2023**, *171*, 108169. [CrossRef]
17. Melnyk, S.A.; Schoenherr, T.; Speier-Pero, C.; Peters, C.; Chang, J.F.; Friday, D. New Challenges in Supply Chain Management: Cybersecurity across the Supply Chain. *Int. J. Prod. Res.* **2022**, *60*, 162–183. [CrossRef]
18. Borchert, H. It Takes Two to Tango: Public-Private Information Management to Advance Critical Infrastructure Protection. *Eur. J. Risk Regul.* **2015**, *6*, 208–218. [CrossRef]
19. Shaked, A.; Tabansky, L.; Reich, Y. Incorporating Systems Thinking into a Cyber Resilience Maturity Model. *IEEE Eng. Manag. Rev.* **2021**, *49*, 110–115. [CrossRef]
20. Gupta, N.; Tiwari, A.; Bukkapatnam, S.T.S.; Karri, R. Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks. *IEEE Access* **2020**, *8*, 47322–47333. [CrossRef]
21. Sobb, T.; Turnbull, B.; Moustafa, N. Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics* **2020**, *9*, 1864. [CrossRef]
22. Meagher, H.; Dhirani, L.L. Cyber-Resilience, Principles, and Practices. In *Cybersecurity Vigilance and Security Engineering of Internet of Everything*; Springer: Cham, Switzerland, 2024; pp. 57–74. [CrossRef]
23. European Union. General Data Protection Regulation. Available online: https://gdpr-info.eu/ (accessed on 6 June 2024).
24. *The NIST Cybersecurity Framework (CSF) 2.0*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024. [CrossRef]
25. Wallis, T.; Dorey, P. Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience. *Energies* **2023**, *16*, 1868. [CrossRef]
26. Lawrence, M.G.; Williams, S.; Nanz, P.; Renn, O. Characteristics, Potentials, and Challenges of Transdisciplinary Research. *One Earth* **2022**, *5*, 44–61. [CrossRef]
27. International Organization for Standardization ISO/IEC 27001:2022. Available online: https://www.iso.org/standard/27001 (accessed on 24 June 2024).
28. National Cyber Security Centre Cyber Essentials. Available online: https://www.ncsc.gov.uk/cyberessentials/overview (accessed on 24 June 2024).
29. System and Organisation Controls. What Is SOC2? Available online: https://soc2.co.uk/soc2 (accessed on 29 April 2024).
30. National Cyber Security Centre. Cyber Assessment Framework. Version 3.2. Available online: https://www.ncsc.gov.uk/collection/cyber-assessment-framework (accessed on 29 April 2024).
31. IET Code of Practice: Cyber Security and Safety. Available online: https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/ (accessed on 20 February 2023).
32. Department for Science, Innovation & Technology. Call for Views on the Code of Practice for Software Vendors. Available online: https://www.gov.uk/government/calls-for-evidence/call-for-views-on-the-code-of-practice-for-software-vendors/call-for-views-on-the-code-of-practice-for-software-vendors (accessed on 7 June 2024).
33. National Telecommunications and Information Administration. Software Bill of Materials. Available online: https://www.ntia.gov/page/software-bill-materials (accessed on 29 April 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.