


Article

Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience

Tania Wallis ^{1,*} and Paul Dorey ² ¹ School of Computing Science, University of Glasgow, Glasgow G12 8RZ, UK² Information Security Group, School of Engineering, Physical & Mathematical Sciences, Royal Holloway, University of London, Egham TW20 0EX, UK

* Correspondence: tania.wallis@glasgow.ac.uk

Abstract: This study describes the implementation of an energy sector community to examine the practice of cybersecurity for operational technology environments and their supply chains. Evaluating cybersecurity from the perspectives of different actors participating in the energy sector, the progress and challenges of operators and suppliers in delivering cybersecurity for the sector are explored. While regulatory frameworks incentivize individual organizations to improve their cybersecurity, operational services contain contributions from many organizations, and this supply chain of activity needs to be influenced and managed to achieve desired security and resilience outcomes. Through collaborations and systems engineering approaches, a reference model is created to facilitate improvements in managing the cybersecurity of supply chains for different actors, including service operators, maintainers, manufacturers, and systems integrators. This study provides an illustration of implementing a common vision of cybersecurity improvement across a community of actors. It utilizes a collaborative framework that has facilitated the co-production of cybersecurity guidance for energy sector participants.

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



Citation: Wallis, T.; Dorey, P. Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience. *Energies* **2023**, *16*, 1868. <https://doi.org/10.3390/en16041868>

Academic Editor: Wencong Su

Received: 22 December 2022

Revised: 2 February 2023

Accepted: 11 February 2023

Published: 14 February 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Critical infrastructure operators are continually challenged by the complexities of considering the security position of their supply chains. This paper describes the implementation of communities of interest in energy supply chain cybersecurity to progress sector-wide approaches to the challenge of overseeing, managing, and influencing supply chains for critical infrastructure.

Operators of critical infrastructure hold responsibility for the impact of cybersecurity events in their operational environment and on the essential services they provide. Regulatory frameworks such as the Security of Network & Information Systems (NIS Regulations) in the UK [1] and the European NIS Directive [2] place cybersecurity expectations on individual organizations, but the operational services deployed utilize components, products, and services coming from multiple supplier companies. Dividing up cybersecurity responsibilities and transferring risk between organizations and between customers and suppliers proves to be a challenge. As a result, regulators further propose to broaden the application of NIS Regulations to organizations supplying critical infrastructure services [3–5]. However, these regulatory tools can only focus on the cybersecurity obligations of individual organizations rather than defining end-to-end security for the technical solutions and services that encompass multiple actors.

This study emphasizes cooperation between interdependent organizations as an essential aspect of cybersecurity governance. It aims to set the foundations for a mutual commitment to agreed cybersecurity objectives and supporting practices. Through addressing the multiple

perspectives of supply chain cybersecurity, it enhances multi-actor partnerships and improves understanding of the operational technology context for cybersecurity.

By implementing a community of interest in supply chain cybersecurity, a pooling of knowledge across the sector enables a broader set of participants to have access to appropriate cybersecurity guidance and best practices that are specific to the operational technology and cyber-physical context of energy services.

1.1. Related Work

Kumar's research on the impact of cybersecurity on operations identifies a critical need for companies to develop a strategy to secure their global supply chains [6]. Ghadge identifies generic research into supply chain cybersecurity and points out the need for more contextualized studies in specific domains [7]. Melnyk calls for more research into cybersecurity across the supply chain and highlights the importance of alignment to a common vision in both a vertical plane, through various actors within an organization agreeing on common goals for cybersecurity, and through horizontal alignment across interdependent organizations working together on common cybersecurity objectives [8].

Messenger [9,10] researches the cultural dynamics at play with the sharing of cybersecurity information across organizational boundaries and proposes the following model of beliefs that are necessary for sharing cybersecurity information:

- I know that my information is important and urgent.
- I know that what I share will help others.
- I know I am trusted by my organization.
- I know how to get the information to the right people.
- I know I can control what happens with what I share.
- I know others will all act with my interests at heart.
- I know others will reciprocate.
- I know I am empowered to share [10].

Rather than information sharing between parties, Borchert [11] recommends joint information ownership and co-production, involving relevant stakeholders by providing a framework to engage them, fostering good relations and trust, and a dedicated focus on developing content together, ideally setting up information co-production per sector to address specifics [11].

Shaked et al. [12] recommend a holistic assessment of cyber resilience using whole systems thinking and proposes "a progression path" to outline how a sector can evolve from one maturity level to the next. This study captures expressions of cyber resilience in the constituents of a sector and in their relationships, and recommends coordinating cyber resilience across a system's constituents rather than relying on self-evaluation by individual entities [12].

Sitton and Reich [13] compare systems engineering methods for improving interoperability across enterprises where existing assets and systems have been developed at different times and places leading to a lack of synchronization. The integration of complex emergent systems is considered from a process design perspective, presenting cross-enterprise processes and information flow as being key to seeing the broader view necessary to lead the way from uncoordinated unsynchronized systems and domains towards new integrated capabilities at the process level. This tends to be hindered by there being no allocated responsibility for defining operational process requirements across organizations. Sitton and Reich recommend viewing 'both ends' by combining top-down strategic thinking and standardization across organizations with a bottom-up evaluation of a continuously evolving environment. This research calls for future projects to demonstrate the planning and management of operational processes to achieve integrated capabilities for complex emergent communities [13].

Carr [14] identifies a "governance gap" in cybersecurity and the need for a coordinating framework, and especially recommends greater engagement between policy and technical communities [14]. Kroger [15] recommends that processes transcend existing organizational

boundaries and follow an “all actors approach” to address the multi-faceted risks of critical infrastructures more holistically [15].

This paper examines the practice of collaboration among energy sector participants and the co-production of guidance to improve cybersecurity assurance of suppliers and their services to the energy sector. It addresses the gaps identified in the literature by providing a contextual study of co-producing cybersecurity guidance with an energy sector community, and by enabling a more integrated cyber capability across different energy sector actors. The collaborative effort also proposes a framework by defining a partnership approach with shared goals for improving cybersecurity across organizational boundaries.

1.2. Issues and Challenges in Supply Chain Cybersecurity Resilience

Contributions to cybersecurity come from a broader set of organizations than individual energy operators. There are many organizations that need to understand their place in critical infrastructure and their role in securing energy services. Extensive supply chains necessitate having some generic approaches in place (usually through adopting published standards) to make the management of vast supply chains achievable. However, a bespoke, individually developed, and blanket approach from companies’ procurement processes has increased workloads for suppliers in responding to each customer’s individual but often all-encompassing question sets that oftentimes are largely irrelevant to the actual component or service they are providing.

Once supply is agreed, some aspects can be controlled by having a security detail within formal agreements and contractual arrangements. However, some aspects (such as changing solutions when threats change) can merely be influenced and so depend on the quality of relations and goodwill between customer and supplier. Awareness and understanding, as far as achievable, of what is outside of an operator’s control or influence is also important, such as sub-contracting and subsidiary tiers in the supply chain or the make-up of software systems. On the other side of the equation, operators know the context (and hence criticality) of the operational environment in which they host supplier products and services and need to effectively communicate the resulting cybersecurity requirements to their suppliers. The quality of relations between operators and their suppliers also contributes to the ongoing resilience of the solution, especially where suppliers need to be engaged during incident response and recovery.

2. Materials and Methods

Topping’s review of contrasting global approaches to managing supply chain cybersecurity calls for more collaborative approaches and more consistent security assurance across borders and sectors [16]. Our paper investigates the feasibility of a common approach to cybersecurity across interdependent organizations. This was progressed through a collaboration with relevant actors from the UK energy sector to jointly design a common and consistent approach to improving the cybersecurity resilience of energy systems.

In 2009 [17], the US Department of Energy and US Department of Homeland Security came up with the idea of helping energy operators in how they specify cybersecurity requirements by providing wording to include in procurement requests and (potentially) in contracts. This was subsequently refined in more focused publications such as one aimed at Energy Delivery Systems [18].

A group of UK electricity and downstream gas companies known as the Energy Emergencies Executive Cybersecurity Task Group (E3CC) saw the value in this approach and in 2018 were supported by the UK Government Department for Business, Energy and Industrial Strategy (BEIS) to work with the Energy Networks Association (ENA) and develop ‘Energy Delivery Systems Cyber Security Procurement Guidance’ [19]. This took the idea of a procurement language and placed it into the context of procurement processes as well as referencing relevant UK and international standards and guidance.

In consideration of the significant growth of new entities in the deployment of energy renewables and more locally managed networks, the group further recognized that grid

stability and reliability could potentially be impacted by systemic cybersecurity risk to multiple distributed energy resources. Adopting the concept of ‘code of connection’ where the energy network defines the rules of connection in order to protect the network, the development of ‘Distributed Energy Resources (DER) Cyber Security Connection Guidance’ [20] was commissioned in 2020. This defines the cybersecurity expectations for distributed energy resources according to their scale and criticality. European energy operators have also produced a Network Code on Cybersecurity clarifying common cybersecurity requirements and defining roles and responsibilities for actors in the European synchronous grid area [21].

The E3CC also saw that carrying out cybersecurity assurance of third parties is becoming common practice for energy operators both at the time of acquiring services or systems and periodically through the life of ongoing contracts. It was recognized that developing, maintaining, and operating such assurance processes are costly and time-consuming. The type of assurance required is similar for every operator, but if everyone ‘does their own thing’ there are inevitably variations in questions and the format and processes used to collect or audit/review information. This diversity of approaches creates a significant overhead for the suppliers being assured.

As a result, the group agreed to a more consistent and potentially shared approach to make the process more efficient for the industry and its supply chain as a whole. Work initially started with a subset of interested operators sharing their internal company methods and questionnaires with a view to creating a common set for the sector, and during the work some key suppliers were also engaged. A collaborative approach ensued involving both operators and suppliers co-producing standard question sets to be used during the procurement process for the assurance of supplier companies. The group then applied an engineering approach by categorizing different parties and co-designing guidance for the assurance of products and services.

2.1. Implementing Energy Sector Partnerships in Supply Chain Cybersecurity

The community of UK energy sector operators in electricity, downstream gas, and oil and gas, as a community considered to have common suppliers and interests, convened to develop the common cybersecurity procurement guidance for operators and eventually establish industry-wide dialogue with the supply chain. The collaboration of this group, working together with members of the supplier community, has improved standardization in cybersecurity to the benefit of suppliers and operators alike.

The initial stages of this work just involved UK energy operators and policymakers. During the process of designing a common approach to supplier assurance, a decision was taken to have ‘validation’ discussions about cybersecurity challenges with key suppliers of systems and services to the energy sector. These meetings proved to be very frank, open, and helpful in understanding the tensions and dynamics of the procurement process and how cybersecurity requirements can be delivered.

For example, suppliers explained how the procurement processes used by some customers could actually inhibit free discussion of cybersecurity concerns if the introduction of additional security context went beyond bidding rules. The suppliers also stressed the importance of a shared responsibility model between suppliers and operators as being key to achieving secure outcomes. The operators took the opportunity to give their opinion that cybersecurity should be an inherent part of any proposal and should not be presented as an optional addition at extra cost.

As a result of working together, the group of suppliers and operators identified that there would be value in an agreement on future standards and approaches. Based on the positive experiences of establishing the collaboration between electricity and gas service operators which formed the E3CC, the operators proposed a Code of Practice and Partnership (CoPP) approach which could form the basis of supply chain cybersecurity assurance and standardization activity in the future.

The CoPP proposal was well received by the collective group of operators and suppliers, and work was started together to agree an initial set of 3 Core Principles for cybersecurity in the supply chain along with 12 supporting Practices shown in Section 3.5. However, despite the interest in collaboration, the group did not gain further traction during 2021. It is interesting to note that although aspiring to work together for a common interest the putative CoPP group differed from the E3CC in at least 2 characteristics. Firstly, it had no resources for facilitation and relied entirely on self-nominating volunteers making time available, and secondly it was formed during the pandemic when physical meetings and opportunities to build personal and social relationships were greatly limited.

2.2. Formation of a Community of Interest Expert Group in Supply Chain Cybersecurity (SCEG)

As a result of the UK National Centre for Cyber Security (NCSC) wishing to promote greater capability in cybersecurity management for the industrial control/operational technology environment, a new group has been established. The initial CoPP work from the energy sector has been used as a catalyst for this cross-sector initiative and has formed an expert group in supply chain cybersecurity. The group aims to progress sector-wide approaches to the challenge of overseeing, managing, and influencing supply chains to critical infrastructure. This includes identifying the progress made so far to determine needs and requirements and provide recommendations on how best to support industry with the challenges experienced in supply chain cybersecurity. The group is exploring the following themes while scoping the need for further guidance and support:

- Establishing commitments to action and maintaining accountability in supply chains.
- Identifying where controls or cooperation/partnerships are required with important suppliers to establish some points of governance within supply chains.
- Reducing the impact and consequences of potential cybersecurity incidents in supply chains to critical infrastructure.

In progressing the new group, the dynamics of collaboration and lessons learnt from the previous groups are being taken into account, and the outcomes and outputs of the new group will be detailed in future work.

3. Results

3.1. Collaborative Energy Community

From its initial establishment as a cybersecurity knowledge-sharing group of operators, the group (now known as E3CC) has been able to work collaboratively, and with the support of their overseeing government department (the Department of Business, Energy and Industrial Strategy), has achieved some key outputs. Table 1 shows the development of the group and its key external achievements beyond knowledge sharing.

Table 1. Development and achievements of E3CC.

Year	Number of Operators	Achievements
2010	6	Formation
2012	12	Government recognition
2013	15	UK-wide risk assessment
2016	18	2nd UK risk assessment Key supplier review event
2018	25	Procurement Guidance [19] Supply Chain Conference
2020	27	DER Cybersecurity Guidance [20] Supply Chain Conference
2021	27	RFI and RFP Standards [22,23]

A review by the Chair of the E3CC outlined the key factors which have contributed to the success of the group; these markedly reflect the views of the literature and can be summarized as:

- A. Invest time in members building personal relationships and trust—including learning together and socializing.
- B. Find common goals that deliver value to all.
- C. Accept that tactical responses will slow down strategic process and plan for contingency.
- D. Think big and look for great (industry-wide) opportunities beyond what single members can achieve.
- E. Do not underestimate the effort required to drive and facilitate the group (it needs some dedicated resources).

3.2. Request for Information

A common information-gathering questionnaire was created by analyzing themes and questions already being posed to suppliers by energy operators. This was tested for completeness by comparison with ISO 27001/2 [24], NIST Cyber Security Framework [25], NIS Regulation Cyber Assurance Framework [26], UK HSE OG86 [27], and guidance from the UK National Cyber Security Centre [28]. A common set of questions was agreed upon which was aimed at the corporate level of suppliers to help create initial company short-lists at the Request for Information (RFI) stage of procurement [22]. The intention is for this Company Initial Questionnaire to become widely adopted for RFIs and thereby make supplier cybersecurity assurance information responses re-useable across different operator engagements.

3.3. Request for Proposal

The cybersecurity status of a company (surveyed by RFI) in terms of its own networks and systems is indicative of corporate security posture but usually falls short of describing the specifics of a service running on different networks and (often) with different cybersecurity management. Therefore, risk-based guidance that focused on particular services or product types was also co-produced to assist the Request for Proposal (RFP) stage of procurement. Figure 1 summarizes the RFI and RFP outputs. The Company Initial Questionnaire in Part 1 provides a general assessment of the cybersecurity capability and posture of a vendor company. Part 2 focuses on the risks relevant to six types of products or services provided and aims to suggest topics for the assurance questions to be asked by operators. For example, security relating to the products and software provided is underpinned by how they are designed and built. RFP questions focus on the relevant risks for the specific product and/or service being provided. Different vendor types bring different cybersecurity risks that can impact the energy operator depending on the activities the vendor performs and the system and data they have access to. Once companies have been short-listed for selection, more specific information is therefore likely to be required about the cybersecurity status of the service or product being procured, e.g., in response to an RFP. This level of service or product cyber assurance may also be performed through the life of a contract.

Unlike a company RFI, it was considered that RFPs will need to be developed for each situation but would benefit from drawing from a common set of references and standards. That formed the basis of the Guidance for Energy Operators for Cyber Security Assurance as part of a Request for Proposal (RFP) [23].

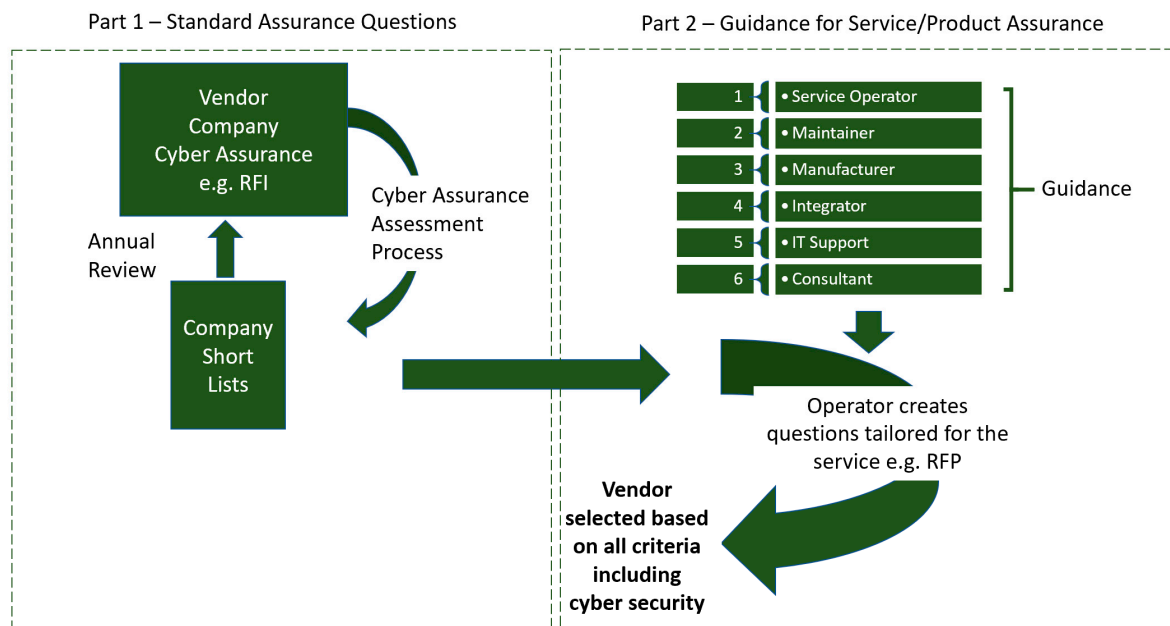


Figure 1. Summary of RFI and RFP outputs.

In the guidance, cybersecurity risks are considered in the context of the different services, and six generic types of service are covered to help operators decide which cybersecurity control topics and standards should be explored. These are:

- A. Service Operator—operates the operational technology (OT) system(s) or closely connected IT-OT system(s) on behalf of the energy company operator.
- B. Maintainer—provides support and maintenance of OT systems.
- C. Manufacturer—provides OT or closely connected IT-OT system/component design, development, and build.
- D. Integrator—provides system integration/configuration/bespoke design.
- E. IT Support Services—support services for IT when acting as an adjunct to OT.
- F. Consultant—provides consultancy such as the assessment of system status including security assessments.

The standards chosen reflect the different risk situations each service might introduce (as shown in Figure 2).

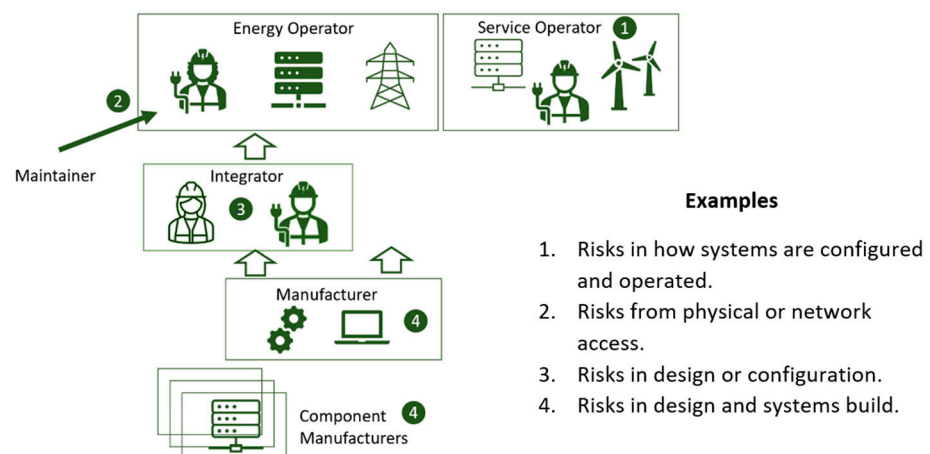


Figure 2. Illustration giving some examples of how different risks can arise in different types of services.

Following the production of the RFI and RFP guidance, the development and delivery of adoption training was progressed to help operators, including their procurement and project professionals, to understand the materials and how to use them.

3.4. *Trust and Partnership in Energy Cybersecurity*

Energy providers recognize that cybersecurity is a risk which they need to manage in order to run resilient energy systems, and they can be required to demonstrate cybersecurity management to comply with regulation. Energy operators therefore have security requirements, some of which they can define themselves, but some need an open dialogue with their systems and service suppliers.

Partnership is therefore essential for effective cybersecurity in the supply chain:

- Partnership addresses information asymmetry where suppliers understand their products in depth, but it is the operator who knows the criticality and context of the application and the impact of potential incidents.
- Partnership recognizes collective and individual roles and responsibilities. For example, vendor products need to have security designed into them, and customer operations need to manage the security of products and how they are used.
- Partnership recognizes fair commercial balance where foundational security is part and parcel of any reliable service or product, and value-added security that brings efficiencies or opportunities such as greater resilience may gain additional reward.
- Partnership enables shared outcomes including working together during incident response and recovery.
- Partnership promotes honesty and transparency in communication to achieve security goals and improve resilience together.

3.5. *Code of Practice and Partnership Model*

The group of suppliers and operators proposed a Code of Practice and Partnership model (CoPP) as a foundational approach to the assurance of supply chain cybersecurity. This work was inspired by other projects producing codes of practice statements on the security goals for OT, IT, and IoT supplier and customer relationships [29–31]. The aim was to create an energy sector CoPP for cybersecurity, to be more specific to the energy industry, and to help guide actions across the supply chain.

Commercial reality in a supply chain requires that for anything to be supplied there needs to be a demand, either naturally in the market or enforced through regulation. To be delivered as a reality, security therefore needs to be something which is genuinely demanded by the customer and not be the subject of ‘lip service’ or something which is removed during negotiation.

Suppliers have expressed concerns that security requirements:

- Are not really a priority in procurement decisions.
- Create a risk of putting suppliers at a competitive price disadvantage on bids or in sustaining an unrealistic product life.
- Are ill-defined and so run the risk of a supplier ‘over-egging’ or underestimating the risk and the matching security requirement.

Operators have expressed concerns that security engagements with suppliers can result in:

- An attempt at raising costs that goes beyond fair return for investment (such as charging bespoke fees for a common security requirement).
- Lack of transparency in the through-life support of security, including unclear or unresponsive reporting on security status.
- Requiring a forced major technology change purely due to security.

Collectively, both operators and suppliers report concern over:

- Too much friction in supply chain cybersecurity assurance, such as numerous different operator questions being posed to suppliers.

- Lack of clarity on which standards and guidance should be adopted.
- Lack of mutual understanding of cybersecurity risks in both current operations and emerging business and technology models.

The Code of Practice and Partnership approach has the goal of trying to create an environment of collaboration to help address the above issues. The CoPP applies to all of the supply chain and has three core principles:

- Basic security is foundational.
- Security and resilience needs collective responsibility.
- Transparency and communication is key.

For each of the above core principles, four partnership practices were identified as shown in Figure 3.

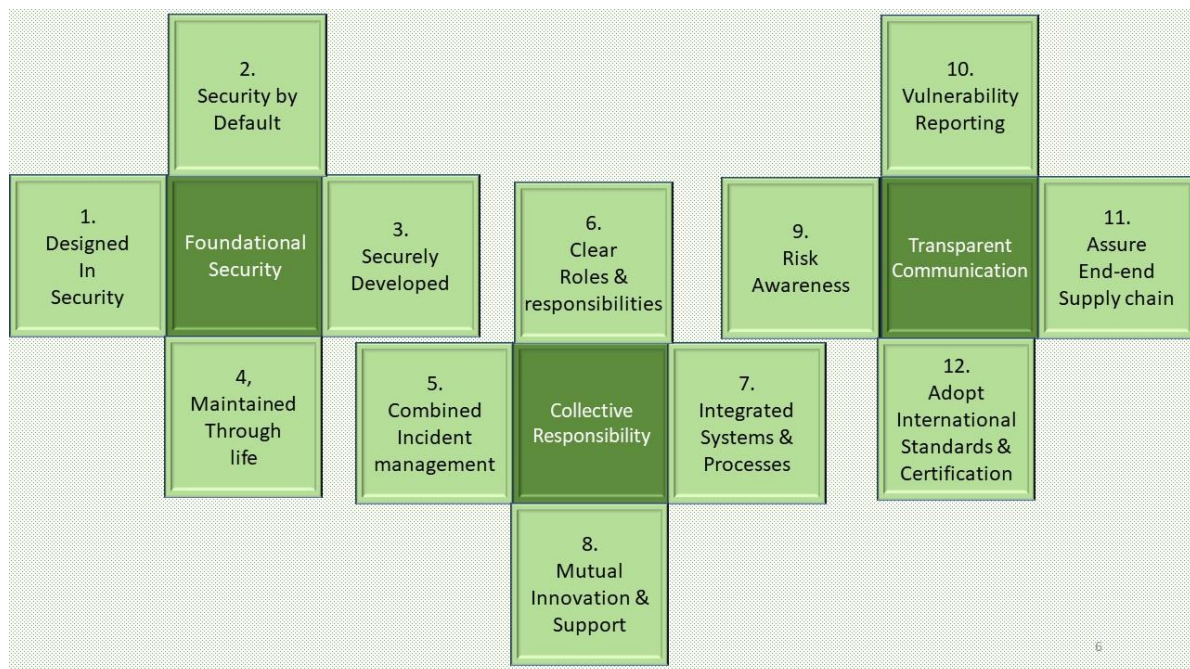


Figure 3. Code of Practice and Partnership Core Principles and Practices.

3.6. Formation of a Supply Chain Expert Group

Since 2022, the implementation of a community of interest in supply chain cybersecurity has been underway, forming a ‘Supply Chain Expert Group’ (SCEG). Amongst other work items, this group is exploring cross-sectoral views on the CoPP and elaborating on the 12 partnership practices identified by the CoPP with more detailed practice statements. Outcomes from this group will be detailed in future work.

4. Discussion

Supply chain cybersecurity is a shared problem which needs shared understanding and partnership to address it. This work with supply chain participants in the energy sector has confirmed that there is a benefit in adopting common cybersecurity assurance standards and approaches in order to reduce unnecessary duplicated work in operators and suppliers. A collaborative approach also achieves a much clearer understanding of cybersecurity risk by all participants and helps overcome information asymmetries in the supply chain.

Whilst a common generic set of questions is useful for a Request for Information (RFI) stage of selecting companies for short-listing, the stage of requesting a proposal (RFP) needs to recognize that there are cybersecurity risks which are specific to the product or service being requested, and so the operator will need to specify the requirements in that context.

Risks can be related to the types of supply of a product or service (e.g., Service Operator, Maintainer, Manufacturer, Integrator, IT Support, and Consultancy), and there are existing industry standards which can be used to define those requirements which can be referred to rather than each customer having to invent their own for each engagement. Suppliers have a strong preference for using existing published standards so that they can standardize design.

To be successful, collaborative groups working on common standards and approaches need a shared mission and must gain individual value from the work. Experience from E3CC, CoPP, and SCEG has shown that these groups must have committed resources for facilitation and be able to develop personal relationships to establish trust.

The common vision and mission of cyber professionals spurs them to donate effort to endeavors such as E3CC, CoPP, and SCEG but will usually require support from their sponsoring organization to collaboratively resource the necessary activity. A combined governance and facilitation capability, which is typically provided by support from government, academia, institutes, or associations, is also essential for such groups to progress significant outputs together.

Author Contributions: Conceptualization, T.W. and P.D.; methodology, T.W. and P.D.; investigation, P.D.; validation, P.D.; resources, T.W. and P.D.; writing—original draft preparation, T.W. and P.D.; writing—review and editing, T.W. and P.D.; visualization, T.W. and P.D.; funding acquisition, T.W. and P.D. All authors have read and agreed to the published version of the manuscript.

Funding: Paul Dorey is retained by National Grid PLC as the facilitator for E3CC and was funded by BEIS to support the development of the RFI and RFP work cited in this paper. This work was funded by the Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS) grant number EP/R022844/1 and EPSRC Impact Acceleration Account EP/X5257161/1. RITICS have provided approval to publish this work.

Data Availability Statement: Not applicable.

Acknowledgments: The support from E3CC members, and energy sector suppliers, during this work is gratefully acknowledged.

Conflicts of Interest: The authors declare no conflict of interest. The funders RITICS and EPSRC had no role in the design of the study; in the collection, analyses, or interpretation of data; or in the writing of the manuscript. BEIS participated in E3CC meetings from a policy perspective during development of the RFI and RFP outputs and oversaw the processes for delivery of the project outcomes referenced.

References

1. Department for Digital Culture Media and Sport. The NIS Regulations. Available online: <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018> (accessed on 29 November 2022).
2. European Commission. NIS Directive. Available online: <https://digital-strategy.ec.europa.eu/en/policies/nis-directive> (accessed on 29 November 2022).
3. Department for Digital Culture Media & Sport. Proposal for Legislation to Improve the UK's Cyber Resilience. Available online: <https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience> (accessed on 29 November 2022).
4. European Commission. Proposal for NIS2 Directive. Available online: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed on 29 November 2022).
5. UK Department for Digital Culture Media & Sport. Consultation Outcome: Government Response to the Call for Views on Proposals to Improve the UK's Cyber Resilience. Available online: <https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/outcome/government-response-to-the-call-for-views-on-proposals-to-improve-the-uks-cyber-resilience> (accessed on 5 December 2022).
6. Kumar, S.; Mallipeddi, R.R. Impact of Cybersecurity on Operations and Supply Chain Management: Emerging Trends and Future Research Directions. *Prod. Oper. Manag.* **2022**, *31*, 4488–4500. [CrossRef]
7. Ghadge, A.; Weiß, M.; Caldwell, N.D.; Wilding, R. Managing Cyber Risk in Supply Chains: A Review and Research Agenda. *Supply Chain Manag. Int. J.* **2019**, *25*, 223–240. [CrossRef]
8. 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]

9. Messenger, M. Why Would I Tell You? Perceived Influences for Disclosure Decisions by Senior Professionals in Inter Organisation Sharing Forums. Master's Thesis, University of London, London, UK, 2005.
10. Messenger, M. Why Would I Tell You? What Makes People Feel Able and Motivated to Share Information? Available online: <https://www.enisa.europa.eu/events/information-sharing-workshop/presentations/mandy> (accessed on 15 November 2022).
11. 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]
12. Shaked, A.; Tabansky, L.; Reich, Y. Incorporating Systems Thinking Into a Cyber Resilience Maturity Model. *IEEE Eng. Manag. Rev.* **2021**, *49*, 110–115. [CrossRef]
13. Sitton, M.; Reich, Y. Enterprise Systems Engineering for Better Operational Interoperability. *Syst. Eng.* **2015**, *18*, 625–638. [CrossRef]
14. Carr, M.; Lesniewska, F. Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance. *Int. Relat.* **2020**, *34*, 391–412. [CrossRef]
15. Kröger, W. Critical Infrastructures at Risk: A Need for a New Conceptual Approach and Extended Analytical Tools. *Reliab. Eng. Syst. Saf.* **2008**, *93*, 1781–1787. [CrossRef]
16. Topping, C.; Michalec, O.; Rashid, A. Contrasting Global Approaches for Identifying and Managing Cybersecurity Risks in Supply Chains. *arXiv* **2022**, arXiv:2208.02244.
17. Homeland Security. Department of Homeland Security: Cyber Security Procurement Language for Control Systems. Available online: https://www.cisa.gov/uscert/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf (accessed on 29 November 2022).
18. Energy Sector Control Systems Working Group. Cybersecurity Procurement Language for Energy Delivery Systems. Available online: https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf (accessed on 29 November 2022).
19. Energy Networks Association. Energy Delivery Systems—Cyber Security Procurement Guidance. Available online: <https://www.energynetworks.org/industry-hub/resource-library/energy-delivery-systems-cyber-security-procurement-guidance.pdf> (accessed on 29 November 2022).
20. Energy Networks Association. Distributed Energy Resources—Cyber Security Connection Guidance. Available online: [https://www.energynetworks.org/industry-hub/resource-library/distributed-energy-resources-\(der\)-cyber-security-connection-guidance.pdf](https://www.energynetworks.org/industry-hub/resource-library/distributed-energy-resources-(der)-cyber-security-connection-guidance.pdf) (accessed on 29 November 2022).
21. ENTSO-E and EU DSO. Network Code on Cybersecurity. Available online: https://www.entsoe.eu/network_codes/nccs/#:~:text=The%20Network%20Code%20on%20Cybersecurity%20aims%20to%20set,responsibilities%20of%20the%20different%20stakeholders%20for%20each%20activity. (accessed on 29 November 2022).
22. BEIS. *Company Initial Questionnaire for Request for Information*; This document is in use by energy sector operators and will be shortly published more widely by BEIS; BEIS: London, UK, 2021; Available online: paul.dorey@csconfidential.com (accessed on 29 November 2022).
23. BEIS. *Guidance for Energy Operators for Cyber Security Assurance as Part of a Request for Proposal*; This document is in use by energy sector operators and will be shortly published more widely by BEIS; BEIS: London, UK, 2021; Available online: paul.dorey@csconfidential.com (accessed on 29 November 2022).
24. British Standards Institution. Information Security, Cybersecurity and Privacy Protection. Information Security Controls. Available online: <https://knowledge.bsigroup.com/products/information-security-cybersecurity-and-privacy-protection-information-security-controls-1/standard> (accessed on 16 December 2022).
25. US National Institute of Standards and Technology. Updating the NIST Cybersecurity Framework—Journey to CSF 2.0. Available online: <https://www.nist.gov/cyberframework/updates/nist-cybersecurity-framework-journey-csf-20> (accessed on 16 December 2022).
26. UK National Cyber Security Centre. NCSC CAF Guidance. Available online: <https://www.ncsc.gov.uk/collection/caf> (accessed on 16 December 2022).
27. UK Health and Safety Executive. *Cyber Security for Industrial Automation and Control Systems (IACS) EDITION 2*; UK Health and Safety Executive: Bootle, UK, 2018.
28. UK National Cyber Security Centre. Supply Chain Security Guidance. Available online: <https://www.ncsc.gov.uk/collection/supply-chain-security> (accessed on 16 December 2022).
29. Siemens. Charter of Trust. Available online: <https://www.charteroftrust.com/> (accessed on 16 December 2022).
30. World Economic Forum. Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain. Available online: <https://www.weforum.org/whitepapers/cyber-resilience-in-the-electricity-ecosystem-securing-the-value-chain> (accessed on 16 December 2022).
31. UK Department for Digital Culture Media & Sport. Code of Practice for Consumer IoT Security. Available online: <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security> (accessed on 16 December 2022).

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.