ENHANCING SUPPLY CHAIN CYBER ASSURANCE IN THE NUCLEAR SECTOR: FINDINGS FROM A COMPREHENSIVE WORKSHOP SERIES

S.N. MELEKWE
Lancaster University
Lancaster, United Kingdom
Email: s.melekwe@lancaster.ac.uk

P. SMITH
Lancaster University
Lancaster, United Kingdom
Email: paul.smith@lancaster.ac.uk

M. ROUNCEFIELD
Lancaster University
Lancaster, United Kingdom
Email: m.rouncefield@lancaster.ac.uk

Abstract

This paper presents an overview of a series of workshops that were focused on supply chain assurance within the nuclear sector. The paper discusses the rationale behind the initiative, emphasizing the importance of supply chain security and cybersecurity within the nuclear industry. Several key areas are explored in the paper, including the development of an overarching strategy, provision of model policies and procedures, maturity assessments, Key Performance Indicators (KPIs) for monitoring risks and performance, the possibility of implementing pilot schemes, and tooling for information exchange. Throughout the paper, we underscore the significance of balancing security with commercial requirements and the need for clear policy directives and procedures. An important theme is the need to engage with a community of interest and gather feedback to enhance supply chain resilience. Additionally, the paper discusses the role of training and toolkit development in equipping stakeholders with the necessary knowledge and resources to implement effective supply chain assurance practices. It also addresses the challenges of data collection and automation. The authors acknowledge the importance of collaboration, scalability, and customization in addressing the unique requirements of each operating company within the nuclear sector. The paper concludes by highlighting the ongoing efforts to refine KPIs for supply chain assessment and emphasizes the need for meaningful and actionable metrics. Overall, this paper offers valuable insights into a holistic approach to supply chain assurance within the nuclear sector and sets the stage for further collaborative efforts in strengthening supply chain security and resilience.

1. INTRODUCTION

The UK civil nuclear industry, a cornerstone of national energy infrastructure, faces unique cybersecurity challenges. In recent years, the nuclear sector has increasingly adopted digital technology to improve operations. However, this digital advancement has led to a significant rise in cybersecurity threats and incidents, affecting all aspects of nuclear security, including the supply chain [1]. The interconnectedness of modern supply chains introduces vulnerabilities that adversaries can exploit, potentially compromising national security and energy reliability. Recognising this, a series of workshops were convened, bringing together stakeholders across the sector to forge a path towards enhanced resilience.

The UK's civil nuclear sector is not only vital for the country's energy security but also represents a significant component of national security. As global incidents such as the SolarWinds [2], NotPetya [3] and more recently the 3CX [4] MOVEit [5] and SIRVA cyber breaches have shown, supply chains can be a weak link in the security armour of critical infrastructure sectors. These events underscore the sophisticated nature of threats facing the nuclear industry, in which the potential consequences of a breach extend far beyond economic loss to include national security risks and public safety concerns.

Given the sector's strategic importance, the initiative to bolster supply chain and cybersecurity represents a proactive and necessary response to a rapidly evolving threat landscape. Cybersecurity in the nuclear sector involves a multifaceted approach, requiring not just the protection of digital assets and critical control systems but also ensuring the integrity and security of the supply chain. This initiative, therefore, seeks to address the dual challenges of maintaining robust cybersecurity defences while ensuring the uninterrupted and safe operation of nuclear facilities. Through a series of workshops and collaborative efforts, stakeholders across the industry have come together as a Community of Interest (COI) working group, to develop a comprehensive strategy that balances operational requirements with the pressing need for enhanced security measures. These stakeholders include Civil Nuclear Sector Chief Information Security Officers (CISOs), Cyber Risk Managers, Contract Security Managers, Supply Chain Managers, Risk Assurance Managers and Academics. This introduction lays the groundwork for discussing the initiatives' components, including strategy development, policy formulation, maturity assessments, and the fostering of a culture of continuous improvement and collaboration within the sector.

2. THE RATIONALE

The rationale to unite key players in mitigating the cyber threats that impact operational efficiency within the Civil Nuclear Industry by advocating for a proactive, comprehensive, and collaborative strategy among the operators, is to synchronize efforts among stakeholders to tackle the critical issue of supply chain cybersecurity. The COI initiative is organised around the following principal areas; firstly, fostering collaboration, ensuring that stakeholders crucial to this dialogue are brought together. The next step is to forge a consensus on a broad-based strategy tailored to this domain. Following this, the creation of adaptable model policies and procedures for stakeholders' use.

The UK National Cybersecurity Centre (NCSC) provides guidance on supply chain security, using attack scenarios to highlight the risks of supply chain attacks, particularly on industrial control systems. These scenarios show how attackers can compromise trusted vendors to insert malicious code, exploiting the trust in these relationships. Such attacks are often sophisticated and can go undetected for long periods [5].

It is important to note that a lot of civil nuclear data is now with suppliers. While many operations have been outsourced, the associated risks cannot be outsourced. There is a need to manage these risks while maintaining a balance between security and commercial requirements.

Some of the driving factors include addressing the ever-increasing risk of a supply chain vulnerability being exploited by attackers. Also, the directive from the UK government Department for Energy Security and Net Zero (DESNZ) [6, 7] as well as meeting other regulatory directives [8].

2.1. Method

The approach includes conducting evaluations to gauge the current state of cybersecurity maturity, pinpointing strengths, and addressing any vulnerabilities promptly. Monitoring risk and performance through KPIs is vital, as it helps to identify where risks are most prevalent among the involved parties.

Additionally, the proposal to launch an adapted version of the Defence Cyber Protection Partnership (DCPP) Cybersecurity Model (CSM) as a pilot programme is reviewed, with the objective of conducting a thorough assessment of suppliers. This programme is intended to integrate within the larger procurement strategy. The DCPP is a collaborative effort spearheaded by the Ministry of Defence (MOD) and industry partners, aimed at fortifying the cyber defences of the defence supply chain [8].

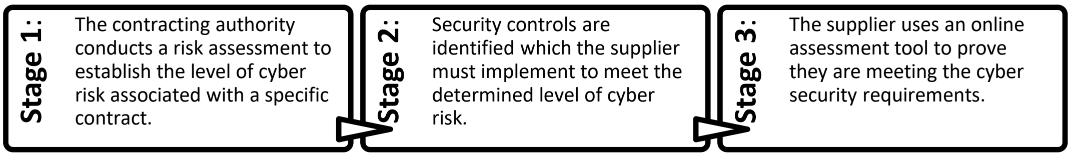
The final segment focuses on the development and exchange of tools designed to streamline and enhance the initiative, complemented by a discussion on the principles underpinning these tools to ensure they effectively capture and interpret essential information.

In the preceding year, this work was initiated after consulting with the industries Supply Chain leads, which included commercial leads from across the industry. Concern was expressed with the varying requirements and processes imposed by different government entities and regulators. A call for clearer, simpler, and more transparent guidelines were made. This feedback was taken seriously and the importance of addressing both cybersecurity and supply chain innovation to meet the industry's mission was recognized.

3. DEVELOPING AN OVERARCHING SUPPLY CHAIN CYBERSECURITY STRATEGY

The UK civil nuclear industry have identified the DCPP's CSM as a potential approach to adopt [9]. The MOD's guidance on assessing and gaining confidence in suppliers aligns closely with what the industry have been doing. UK Government entities are converging around this approach [10], and the civil nuclear industry is supportive of it as it is closely aligned with the NCSC supply chain guidance. It is also a tested model, having been implemented by the MoD since 2017 with over 57,300 contracts processed in the last five years [11]. Additionally, it should provide consistency, clarity and transparency for commercial, procurement and cyber teams dealing with supply chains, by providing a repeatable processes and procedures aimed at improving efficiency and providing proportionate protection of supply chain risk and process to enable swift onboarding of suppliers, potentially saving time and costs. It also enables simplified risk reporting on contracts and suppliers and offers increased possibility for automation for civil nuclear industry and suppliers.

The DCPP is a joint MOD and industry initiative to improve the protection of the defence supply chain from the cyber threat. In the DCPP CSM shown in Fig. 1, the contracting authority initiates the Stage 1 risk assessment through a questionnaire, categorising project risk and complexity into five Cyber Risk Levels, ranging from Not Applicable to High. In Stage 2, the authority assigns a Cyber Risk Level to each contract, requiring suppliers to adhere to specified Cyber Risk Profiles, with the possibility of implementing additional controls in collaboration with an MOD Cyber Defence and Risk (CyDR) representative. Stage 3 involves the contractor submitting evidence for review and potential acceptance by the authority, facilitated by an online tool under development to streamline the process.



Stage 1: The contracting authority conducts a risk assessment to establish the level of cyber risk associated with a specific contract.

Stage 2: Security controls are identified which the supplier must implement to meet the determined level of cyber risk.

Stage 3: The supplier uses an online assessment tool to prove they are meeting the cyber security requirements.

Fig. 1. DCPP Cybersecurity Model (CSM)

The policy initiative adopted by the COI working group is crucial for enhancing the safety and security of the civil nuclear sector, going beyond compliance to incorporate best practices influenced by the UK government Department for Energy Security and Net Zero (DESNZ) goals and advice from regulatory and cybersecurity bodies. The civil nuclear industry looks to develop a succinct policy statement for executive endorsement and detailed guidance documents, supported by procedures that align with the DCPP for effective supplier management. This effort is part of a broader governance framework designed to address significant risks, seeking stakeholder feedback to ensure these policies and procedures are effective and aligned with the UK public sector objectives. The comprehensive strategy includes supplier assessments and cyber risk management, highlighting an approach to cybersecurity and supply chain protection.

3.1. Adapting The Model

The DCPP CSM is adapted to suit the nuclear industry for the Pre-Contract Phase. Fig. 2 shows the model adapted for the contracting authorities with the civil nuclear industry.

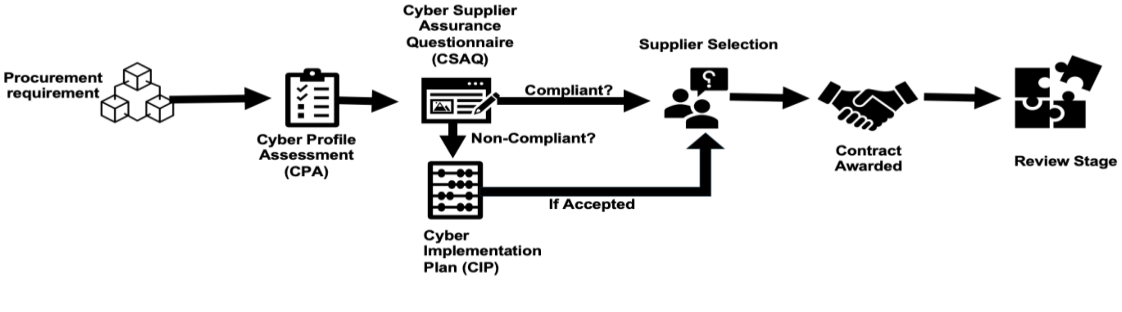

Procurement requirement
Cyber Profile Assessment (CPA)
Cyber Supplier Assurance Questionnaire (CSAQ)
Compliant?
Non-Compliant?
Cyber Implementation Plan (CIP)
If Accepted
Supplier Selection
Contract Awarded
Review Stage

Fig. 2 Adapted Cybersecurity Model for civil nuclear contracting authorities.

The process can be summarized, as follows. The Contract Lead at the Contracting Authority performs a Cyber Profile Assessment (CPA) to gauge the cyber risk associated with a particular contract and to determine its Cyber Risk Profile. Suppliers interested in the contract are required to fill out a Cyber Supplier Assurance Questionnaire (CSAQ). The Contracting Authority then assesses these questionnaires, along with any provided evidence, if the supplier is compliant then it passes to the selection stage; otherwise, a Cyber Implementation Plan (CIP) is put in place, as part of the contract award process, which incorporates standard security clauses from the Contracting Authority. Upon contract award, these standard clauses, along with any specific requirements from the CIP, are included. This is followed by a Review Stage.

The DCCP model uses six questions in conducting the CPA [11]. In adapting this, it is agreed that a seventh question should be added to identify Sensitive Nuclear Information (SNI). So, the questions on the CPA would be based on the below seven areas to be adapted by the contracting authority:

(a) **Any Identifiable Information processed:** Refers to whether the contract involves the processing of any contracting authority's identifiable information or the generation of such information by the supplier.
(b) **Supplier / Electronic storage / processing:** Indicates if the supplier digitally stores or process any contracting authority's data.
(c) **Overall classification:** The highest level of classification of the information and handling requirements associated with the overall contract.
(d) **Classification passed to subcontractor:** The security level of any data stored or processed by any subcontractors involved if any.
(e) **Personal Information:** Involves checking if the contract requires the processing of personal data.
(f) **Remote connectivity into network:** Indicates if the contract allows the supplier network access to the contracting authority.
(g) Pilot seventh question: **Does the contract handle SNI:** Queries if the contract deals with Sensitive but Nuclear Information (SNI), which requires special handling.

The CSAQ aims to unify the collection of corporate information across the civil nuclear industry by establishing a common framework that includes both obligatory information and optional exemption criteria. It allows the contracting authority to tailor the questionnaire with specific questions relevant to the project. The CSAQ is designed to assess the status of a supplier's compliance and competence, such as existing security measures, rather than potential future conditions. Concurrently with the CSAQ, or as part of the Invitation to Tender (ITT), the contracting authority will pose forward-looking 'Technical' questions to gauge how the bidder plans to fulfil the contract's requirements for goods, services, or works. The fundamental goal of the CSAQ is to determine if a bidder is a suitable and trustworthy entity with which the contracting authority can envisage a professional relationship.

In the envisioned tool, the Supplier Questionnaire (SQ) comes pre-populated with over fifty compulsory questions, while procurement professionals have the capability to append project-specific queries. The content of the SQ and the ITT Technical Envelope, which may contain templated and additional bespoke questions, is determined by the contracting authority in collaboration with their commercial team. The format of these questions may vary, offering both pass/fail or scored options. Bidders are obliged to respond to all inquiries and, when requested, substantiate their self-declared statements with evidence. The CSAQ is integrated within the SQ/ITT Technical envelope as a critical pass/fail item, linked to the risk level established in the CPA. Bidders are provided with the relevant CSAQ questions to comprehend what will be expected of them should they advance to the status of preferred supplier. A failure to meet the CSAQ standard precludes further participation in the procurement process. Upon selection as the preferred supplier, and before the final contract award, the bidder must satisfactorily complete the CSAQ and furnish any necessary evidence, such as certifications or policy documents. The cybersecurity team then reviews these submissions, determining one of three outcomes: a full pass where all criteria are met, a conditional pass requiring additional action and a cyber implementation plan, or a failure if the evidence does not demonstrate compliance with the set criteria.

4. MATURITY ASSESSMENTS AND KEY PERFOMANCE INDICATORS

Maturity assessments play a crucial role in establishing a baseline for cybersecurity readiness [12], while KPIs offer quantifiable metrics to gauge effectiveness over time [13]. Together, they enable a data-driven approach to cybersecurity, facilitating targeted improvements and strategic decision-making. It was agreed that operating companies within the industry should conduct a uniform maturity assessment. To help establish a baseline for the industry, questionnaires were distributed to operating companies to assess their current Cyber Supply Chain Risk Management (C-SCRM) practices. Upon receipt of the responses, a meeting was held with representatives from these companies to delve deeper into the information and evidence provided in the initial questionnaire responses. Following these discussions, a concise summary highlighting the yes/no outcomes and qualitative insights was shared with the operating companies for validation, ensuring the report accurately reflects their current C-SCRM status. Finally, an overarching *confidential* report for the industry was compiled, summarising the collective findings from the operating companies. This report identifies immediate opportunities for improvement, strengths, and weaknesses within the industry, offering an overview of the assessment results.

The COI highlights that understanding board expectations for KPIs and Key Risk Indicators (KRIs) requires direct conversations, facilitated by structured methods like the Responsible, Accountable, Consulted, and Informed (RACI) matrix [14] to clarify roles and align interests. A suggested approach involves directly asking the board about their cybersecurity KPI preferences, advocating for communication that targets specific, actionable metrics essential for strategic oversight and decision-making.

Furthermore, the emphasis is on practical KPIs that identify significant changes and trends, focusing on areas needing urgent action to mitigate vulnerabilities, rather than just statistical data lacking in-depth analysis. This perspective underlines a preference for actionable intelligence. Conversely, discussions on KRIs suggest a strategic layer where the board prioritises information on exceptions or anomalies outside acceptable ranges. This approach differentiates between everyday metrics and critical risk indicators, highlighting the COI's focus on governance and risk management through precise, impactful information that enhances organisational control and resilience.

KPIs will be predominantly generated from data obtained throughout the supplier assessment process. This data will be systematically collected utilizing standardized Excel templates, designed for ease of aggregation and consolidation. Such a methodology facilitates the seamless integration of data into real-time dashboards, specifically utilising tools like PowerBI, to provide a dynamic analytical platform [15, 16]. Efforts will be made to minimize additional data requests from Operating Companies and suppliers to ensure efficiency and reduce operational burden.

Furthermore, these KPIs will be anchored on well-defined metrics, offering the capability to aggregate and interpret data at various hierarchical levels through real-time dashboards, courtesy of advanced analytical tools, thereby enabling stakeholders to derive deeper insights with the requisite granularity. This approach underscores the strategic application of business intelligence tools to enhance decision-making processes within the supplier assessment framework. Suggested KPIs include percentage of CIPs completed relative to the number of CSAQs and tender, number of contracts with up-to-date RACI information, percentage of suppliers reviewed within stipulated review window timeframe.

5. TRAINING AND TOOLKIT DEVELOPMENT

Tooling plays a pivotal role in the UK civil nuclear industry for several key reasons. Firstly, it reduces the reliance on labour-intensive processes, enabling suppliers to enhance their self-sufficiency with minimal external intervention. This is crucial for streamlining operations and fostering a more autonomous supply chain ecosystem. Additionally, advanced tooling facilitates the generation of more insightful Management Information (MI), crucial for effective reporting and the development of comprehensive dashboards. Integration capabilities of these tools with other systems significantly reduce redundant data entry, thereby increasing efficiency. Improvements in cyber-savvy behaviours are also a direct benefit of sophisticated tooling, which not only enhances the security posture but also adds value to external systems, adopting a consistent and standardised approach to tooling across the Civil Nuclear Industry, in alignment with guidelines from DESNZ, ONR, NCSC, NIST, and DPCC, ensures a unified strategy that strengthens the sector's resilience and operational efficiency.

A toolkit was created to guide contracting authorities through each of the five steps from the NCSC, along with the detailed instructions to roll out the strategy, policy, and procedures effectively. The primary focus is on the specification, requisition, procurement, and award of contracts to new suppliers.

Within the context of the toolkit, the RACI framework—encompassing roles of being Responsible, Accountable, Consulted and Informed—serves as a foundational pillar for delineating duties and establishing a systematic escalation process for incidents involving supplier systems. This framework not only clarifies procurement responsibilities but also extends to ensuring all stakeholders are cognisant of their roles, particularly in scenarios where supplier vulnerabilities may compromise organisational integrity. The criticality of implementing a clear, predefined escalation protocol cannot be overstated; it necessitates the identification of responsible individuals or departments for immediate notification upon detection of a supplier issue. A comprehensive procedural blueprint, addressing key questions regarding the initiation of contact, the sequence of escalation, and the delineation of responsibilities among suppliers, is imperative for pre-emptive planning. This approach underscores the necessity of having robust, actionable strategies in place, rather than resorting to ad hoc measures in the wake of security breaches, thereby reinforcing the contracting authority's resilience and response efficacy to supply chain threats.

As an example of a RACI Model, the category manager or procurement role is responsible for ensuring the completion and documentation of the CPA. They are the custodians of the procurement process. The client lead (the one receiving the service) or their delegate, must understand the risks and ensure these are mitigated, consulting technical and domain experts when needed. The client lead is the key accountable role. The CISO is consulted as required, especially for complex or technical matters. Key stakeholders, those impacted or needing to be aware, are informed. The level of consultation and information varies with the complexity of the scenario. Most scenarios will be straightforward, aligning with existing processes, but understanding how and when to consult and engage is essential.

5.1. Training Toolkit

Training programme toolkits equip stakeholders with the necessary knowledge and resources to implement robust cybersecurity measures. These resources are critical for raising awareness and fostering a proactive cybersecurity posture across the supply chain.

Results from maturity assessment that was conducted revealed that while IT security awareness training is universally administered to employees, it typically lacks a dedicated focus on cybersecurity within the supply chain. Additionally, procurement personnel are not receiving formalized instruction on Supply Chain Cybersecurity. Where such training does exist, it tends to be delivered in an informal and sporadic manner rather than through a structured program.

The cyber supply chain training toolkit is designed to establish a uniform cybersecurity baseline among all team members. This ensures that everyone comprehends the essential requirements and desired outcomes for minimizing the operational impact of cyber threats within the supply chain. It aims to provide a deep understanding of the specific cybersecurity threats that are pertinent to individual roles, clarifying the significance of supply chain security and its applicability to one's duties. Moreover, it delineates each team member's responsibility in identifying and mitigating cyber risks, offering a comprehensive overview of the available support mechanisms and how to utilise them effectively.

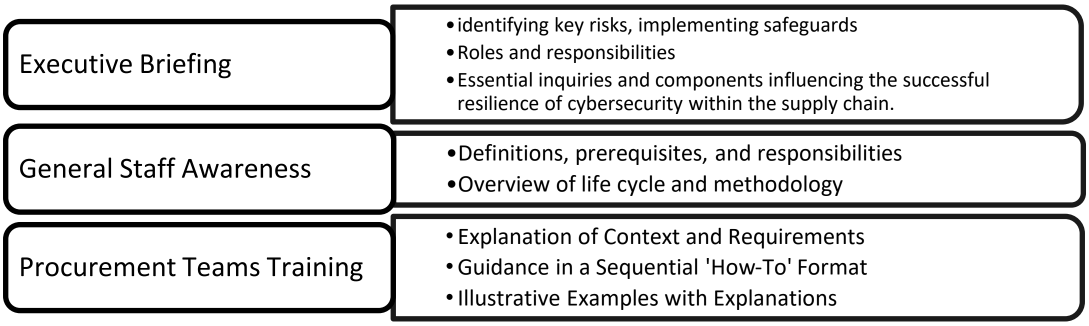

Executive Briefing
• identifying key risks, implementing safeguards
• Roles and responsibilities
• Essential inquiries and components influencing the successful resilience of cybersecurity within the supply chain.
General Staff Awareness
• Definitions, prerequisites, and responsibilities
• Overview of life cycle and methodology
Procurement Teams Training
• Explanation of Context and Requirements
• Guidance in a Sequential 'How-To' Format
• Illustrative Examples with Explanations

Fig. 3 Proposed training model.

6. PILOT SCHEMES

The introduction of a pilot schemes allows for real-world testing of proposed strategies. Tenders for eleven contracts were put through the pilot scheme at some of the contracting authorities. Insights where gained that led to some proposed refinement of the process as below.

- There was a notable lack of uniformity in the information provided across various tenders.
- Assessments could not be carried out without engagement with the procurement team.
- In certain instances, the procurement team lacked the requisite knowledge to fully execute the assessments.
- It was challenging to determine the classification level of the information that was to be processed.
- Completion of some Cyber Risk Profiles (CRPs) was not possible without guidance and support from the CISO team.
- None of the contracts reviewed were assigned a Cyber Profile Assessment (CPA) score in the Moderate to High range.

The learnings derived from the findings indicate several areas for improvement in the process:

(a) **Process Standardisation:** A consistent process to assess contracts is essential for ensuring that all contracts are evaluated against the same criteria, reducing variability, and increasing reliability in the risk assessment process. Establishing a standardised procedure would also facilitate training and onboarding for team members and ensure that all relevant risks are identified and managed uniformly.

(b) **Tender Documentation:** The fact that additional input was required beyond the available tender documentation suggests that current documentation may be insufficient in detail or scope. To complete CPAs effectively, tender documents should include comprehensive information about cybersecurity expectations, standards, and requirements. This may require revising the tender process to ensure that documentation is thorough and adequate for risk assessment purposes.

(c) **Collaborative Requirement:** CPAs cannot be unilaterally completed by Procurement alone but require input from multiple stakeholders. This points to the need for a multi-disciplinary approach to risk assessment, involving stakeholders such as client leads who have a deep understanding of the business needs and can provide context-specific information that may influence the risk profile of a contract.

(d) **CISO Team Involvement:** The involvement of a CISO representative is crucial, particularly in instances where CRPs are challenging to determine. Their cybersecurity expertise can provide the necessary guidance and support to ensure that risk assessments are accurate and that any identified risks are properly managed. This learning emphasises the need for cybersecurity leadership in the procurement process and the value of their strategic input.

(e) **Contract Pool:** The expectation of a small population of contracts with a Moderate to High CRP suggests that high-risk contracts may be rare.

The overarching theme from these learnings is that the organization needs to enhance the collaborative efforts between procurement, cybersecurity experts, and client leads to ensure a holistic and accurate cyber risk assessment process.

7. BALANCING SECURITY WITH COMMERCIAL REQUIREMENTS

A key theme is the need to integrate cybersecurity measures without unduly hindering commercial operations. Policies and procedures are designed to be flexible, allowing for customization to meet the unique needs of each entity within the supply chain.

In adapting the framework to the specific needs of the civil nuclear industry, there's a necessity to account for the application of various frameworks at different organisational tiers. When customising an existing framework, it is recognised that not all standard questions may be relevant; such scenarios will necessitate the inclusion of project-specific questions within the Invitation to Tender (ITT), extending to dynamic purchasing systems and marketplaces. Suppliers passing all the CSAQ items may advance to the subsequent phase of the tendering process. For responses that require further attention, a determination will be made regarding their acceptability without overhauling the entire submission. Minor modifications that can be addressed before contract initiation may be permissible. Nevertheless, a failure in the CSAQ results in the supplier's discontinuation from the current procurement exercise. It is imperative to maintain an efficient process, tailoring inquiries to align with the associated risk level of the contract and avoiding the creation of undue impediments.

The utility of the toolkit, as discussed in relation to the CSAQ form, is primarily contingent upon its outputs being congruent with existing risk management processes within contracting authorities and their business units. Such alignment is critical; when presenting a supplier as a potential risk to security and risk directors, it is imperative to contextualise this within the broader spectrum of risks they are concurrently managing. However, adherence to the industry-sanctioned approach is paramount. Unnecessary innovation within the toolkit that may disrupt established methodologies must be avoided and consensus achieved through COI working groups. It is essential to judiciously evaluate existing frameworks and uphold prior agreements, thus ensuring that cyber supply chain risk assurance efforts complement and enhance the current risk management ecosystem rather than introducing redundant or conflicting elements.

8. COMMUNITY ENGAGEMENT AND FEEDBACK

Engaging with a community of interest for feedback is vital for refining practices and ensuring that policies and procedures remain relevant and effective. This iterative process encourages a culture of continuous improvement and resilience-building [17].

The importance of the COI working group within the civil nuclear industry, particularly in the context of supply chain cybersecurity, is multifaceted and substantial. The COI working group serves as a cornerstone for collaborative efforts, facilitating the sharing of best practices, insights, and strategies across various stakeholders. It enables the industry to collectively address the myriad challenges posed by cybersecurity threats in a coherent and unified manner.

By leveraging the collective expertise and resources of its members, the COI aims to enhance the overall resilience of the civil nuclear supply chain against cyber threats. It plays a pivotal role in the dissemination of knowledge, ensuring that all parties, from suppliers to contracting authorities, are equipped with the necessary understanding and tools to mitigate risks effectively. This is exemplified by the standardisation of procedures, such as the quick adoption of the CSAQ and CPA, which benefits from the COI's input and oversight.

Furthermore, the COI acts as a conduit for aligning cybersecurity practices with broader governmental and regulatory frameworks, thereby reinforcing the sector’s compliance with national security standards and contributing to the national objective of maintaining a secure and reliable civil nuclear infrastructure. It ensures that cybersecurity measures are not isolated initiatives but are integrated with existing risk management processes, thereby aligning with the industry’s overarching security objectives.

Through initiatives such as training toolkits and cyber assessments, the COI empowers entities within the civil nuclear sector to not only understand their role in cybersecurity but also to actively participate in the identification and mitigation of potential cyber threats. This collaborative environment fosters a culture of continuous improvement and innovation, ensuring that the civil nuclear industry remains agile and responsive to the evolving cybersecurity landscape.

In essence, the COI is instrumental in orchestrating a synchronised approach to cybersecurity within the civil nuclear supply chain, advocating for a balance between robust security measures and the practical commercial realities of the industry. Its role is vital in upholding the security of the civil nuclear sector and, by extension, the broader public interest.

9. ADDRESSING DATA COLLECTION AND AUTOMATION CHALLENGES

The COI acknowledges the challenges of data collection and automation, striving to develop scalable solutions that can accommodate the diverse and dynamic nature of the nuclear supply chain.

Addressing data collection and automation challenges in nuclear supply chain cybersecurity is a multifaceted effort that touches on several aspects of the supply chain management within the civil nuclear sector. It is clear that standardised data collection is paramount. The use of tools such as the CSAQ provides a consistent framework for capturing company information and assessing cyber risk, essential for establishing a baseline understanding of the security posture across the supply chain.

However, challenges arise due to the variability in the information provided across tenders and the need for project-specific questions that may not be covered by existing frameworks. This indicates a gap that automation can address. By implementing systems that can pre-load standardized questions and allow for the easy integration of additional, bespoke queries, the contracting authority can ensure that data collection is both comprehensive and adaptable to the specific needs of each contract. The goal is to have a streamlined, efficient process that aligns with other risk processes within the contracting authorities and businesses, thereby enhancing the decision-making process.

Automation is also key in overcoming the labour-intensive nature of traditional data collection and assessment methods. The development of an online tool that can facilitate the submission of evidence by contractors and automate the initial stages of the assessment process would represent a significant step forward. This tool should ideally integrate with existing systems to prevent duplication of data entry and allow for real-time updates to dashboards and reports.

Furthermore, addressing automation challenges extends to the training provided to staff. The findings that current training on supply chain cybersecurity is informal and ad-hoc suggest that there is room for developing more structured and automated training modules. These could be regularly updated to reflect the latest threats and best practices, ensuring that all employees, especially those in procurement and IT security roles, have a consistent and up-to-date understanding of the cyber risks specific to the supply chain.

Finally, automation must be approached with care to ensure that it complements and does not replace the industry-agreed upon approaches and frameworks. Any new tools developed should work in concert with the established protocols and guidelines from organizations such as the Office for Nuclear Regulation and the National Cybersecurity Centre.

10. CONCLUSION

In conclusion, the paper encapsulates the collective endeavour within the UK civil nuclear sector to bolster supply chain cyber assurance through a series of COI workshops. It underlines the critical balance between security measures and commercial operations, advocating for clear policy directives and collaborative engagement across the civil nuclear industry. The paper also emphasizes the role of standardized tools like the CSAQ in streamlining cybersecurity assessments, alongside the pivotal contribution of training and toolkit development in equipping stakeholders. It advocates for a unified approach to tackling cybersecurity challenges, leveraging automation and data collection enhancements to improve efficiency and resilience. Through these concerted efforts, the paper sets a foundation for ongoing collaboration and innovation in strengthening the sector's defence against cyber threats, highlighting the significance of actionable KPIs and the value of community feedback in refining cybersecurity practices.

The authors recommended that the COI working group should define a supply chain mapping strategy across all contracting authorities as this is pivotal for identifying and managing critical suppliers, thereby enhancing resilience and risk mitigation within the supply chain. This strategy recommendation will involve the contracting authorities diversifying critical suppliers, when possible, to prevent dependencies on a single source, thus avoiding potential failure points. By maintaining a comprehensive inventory of suppliers and their subcontractors, organizations can achieve effective risk management, ensure transparency, and uphold compliance with regulations.

Such an inventory not only facilitates performance monitoring and identifies dependencies but also strengthens communication and collaboration within the supply chain. Regular updates to this inventory are essential to adapt to changes and maintain its relevance, particularly in addressing cybersecurity risks. Utilizing technology tools for supply chain management can further streamline the tracking and organization of supplier information, making it a foundational practice for building a resilient and efficient supply chain capable of navigating the complexities of modern business environments.

ACKNOWLEDGEMENTS

Solomon Melekwe’s research is supported by ENERGUS and the Nuclear Decommissioning Authority (NDA). The authors extend their appreciation to all team members and colleagues for their invaluable input and support throughout the course of this study.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY - IAEA, Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain, (2022).

[2] MARTÍNEZ, J., DURÁN, J.M., Software supply chain attacks, a threat to global cybersecurity: SolarWinds’ case study, International Journal of Safety and Security Engineering 11 5 (2021) 537.

[3] BRUMFIELD, C., 5 years after NotPetya: Lessons learned, Channel Asia (2022).

[4] CONSTANTIN, L., 3CX hack highlights risk of cascading software supply-chain compromises, CSO (Online) (2023).

[5] CORREIA, M., MOVEit hack ignites worry about fiduciary responsibility, Pensions & Investments 51 13 (2023) 3.

[6] DEPARTMENT FOR ENERGY SECURITY & NET ZERO (DESNZ), CIVIL NUCLEAR: ROADMAP TO 2050, (2024).

[7] DEPARTMENT FOR BUSINESS & TRADE, Critical Imports and Supply Chains Strategy, https://www.gov.uk/government/publications/uk-critical-imports-and-supply-chains-strategy/critical-imports-and-supply-chains-strategy-html-version, https://www.gov.uk/government/publications/uk-critical-imports-and-supply-chains-strategy/critical-imports-and-supply-chains-strategy-html-version.

[8] OFFICE OF NUCLEAR REGULATION (ONR), Security Assessment Principles for the Civil Nuclear Industry, (2022).

[9] OFFICE FOR NUCLEAR REGULATION (ONR), ONR Technical Assessment Guide Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services, (2023).

[10] NCSC, How to Assess and Gain Confidence in Your Supply Chain Cyber Security, https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security.

[11] DEFENCE CYBER PROTECTION PARTNERSHIP, Defence Cyber Protection Partnership: Guidance, https://www.gov.uk/guidance/defence-cyber-protection-partnership#news.

[12] CIUREA, C., BOJA, C., POCATILU, P., DOINEA, M., “Cyber Security Maturity Model for Critical Infrastructures”, Education, Research and Business Technologies, Smart Innovation, Systems and Technologies, Vol. 276, Springer, Singapore (2022) 225–236.

[13] PATIDAR, A., SHARMA, M., AGRAWAL, R., SANGWAN, K.S., Supply chain resilience and its key performance indicators: an evaluation under Industry 4.0 and sustainability perspective, Management of environmental quality 34 4 (2023) 962.

[14] COSTELLO, T., RACI-Getting Projects “Unstuck”, IT Prof 14 2 (2012) 64.

[15] RHODES, J.M., Creating Business Applications with Microsoft 365: Techniques in Power Apps, Power BI, SharePoint, and Power Automate, book, Second edition., Apress L. P, Berkeley, CA (2022).

[16] DING, D., Transitioning to Microsoft Power Platform: An Excel User Guide to Building Integrated Cloud Applications in Power BI, Power Apps, and Power Automate, book, 1st ed., Apress L. P, Berkeley, CA (2023).

[17] NIK-BAKHT, M., EL-DIRABY, T.E., Communities of Interest-Interest of Communities: Social and Semantic Analysis of Communities in Infrastructure Discussion Networks, Computer-aided civil and infrastructure engineering 31 1 (2016) 34.