Implementing the NIS Directive, driving cybersecurity improvements for Essential Services

Tania Wallis
School of Computing Science
University of Glasgow
Glasgow, UK
tania.wallis@glasgow.ac.uk

Prof. Chris Johnson
School of Computing Science
University of Glasgow
Glasgow, UK
christopher.johnson@glasgow.ac.uk

***Abstract*— A review by the National Audit Office of the National Cyber Security Programme recommended a more robust performance framework, to understand the impact of the Programme and to focus activities going forward. The Directive on security of network and information systems (the NIS Directive) has placed responsibility for essential aspects of supply chains on Operators of Essential Services (OES). Our dependence on international supply chains also requires a performance framework to assist cybersecurity improvements in this area. The following sections describe work to investigate the implementation of the NIS Directive by Competent Authorities (CA) and OES and proposes a framework to monitor performance across interdependencies. This is to enable development of a more effective set of performance metrics to guide interventions and improvements in cybersecurity for critical infrastructure.**

Keywords*—cybersecurity, resilience, critical infrastructure, metrics, supply chains*

I. Introduction

A review by the National Audit Office looking at the progress of the National Cyber Security Programme has recommended a better understanding of the areas of greatest impact and importance, to focus activities during the remainder of the Programme and to develop a new approach to transition beyond the current Strategy and Programme [1].

There have been challenges with managing programme risks due to not having in place a robust performance framework. The Cabinet Office reported low confidence in the evidence behind metrics that were intended to track performance across the National Cyber Security Programme. The National Audit Office showed either low confidence or moderate confidence in the strategic outcomes being achieved, for those they were able to publicly report progress on. With regard to Critical Infrastructure (CI) fewer than 80% of the CI projects were expected to be achieved [1].

The overarching themes of the National Cyber Security Programme are:

- Deterrence – detection and countermeasures, reducing impact of cyber events.
- Defend – protection and incident response, guidance regulation and incentives to manage cyber risks.
- Develop – building expertise and capability.
- International activity – partnerships, increased consensus & capability, responsible behaviour.
- Governance – policies, organisations, structures for effective response to the threat [1].

The Defend theme includes Critical National Infrastructure activities which the Cabinet Office oversees, while the Department for Digital, Culture, Media and Sport (DCMS) hold responsibility for all other businesses under this objective [1]. The overarching governance of this cross-government approach, to maximise effectiveness, requires careful measurement to understand its actual impact.

The Directive on security of network and information systems (NIS Directive) was transposed into UK law in May 2018 in response to EU aims to raise the level of cyber security across member states [2]. It brings a focus to the resilience of our essential services in Energy, Water, Transport, Health & Finance.

Implementing the NIS Directive began with the National Cyber Security Centre (NCSC) defining a set of principles, shown in Figure 1, to aid decision making in securing essential services and a Cyber Assessment Framework (CAF) indicating best practices [2].

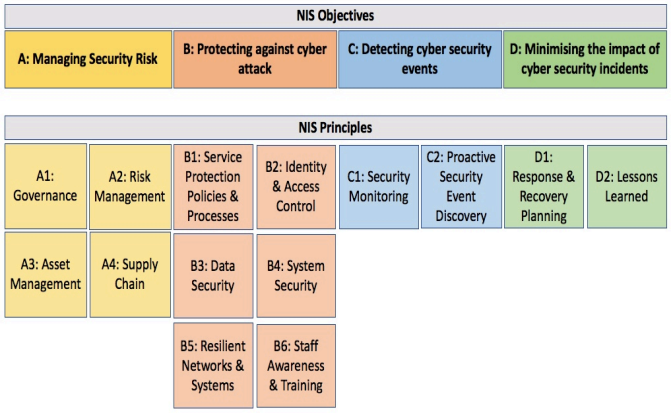

Figure 1 NIS Objectives

The CAF has been adapted for each sector by working with the sectoral Competent Authorities (CA) [2]. The Operators of Essential Services (OES) have been obliged to complete self-assessments against the CAF. This has resulted in a body of knowledge and evidence across several Critical Infrastructure sectors on the cyber security level of our essential services. This can form a basis for future decision making on cybersecurity improvements [3].

II. Methodology

At a more generic level, this project explores the nexus between evidence-based research methods for science and engineering and public policy. It describes the use of qualitative methods, based on focus groups, interviews and active research tools to identify putative metrics with which to assess the comparative strengths of NIS implementation both across sectors within the UK and more widely throughout our international supply chains. It demonstrates the importance of cyber security researchers engaging with policy to aid CAs and NCSC in meeting the expectations of lead government departments. The project is engaging with three different Critical Infrastructure sectors, through semi-structured interviews with OES and CA in those sectors, as well as meetings with NCSC and lead Government Departments, to assess the progress of the NIS Directive. This engagement includes action-based research to assist stakeholders, where appropriate, to meet their objectives within the National Cyber Security Strategy.

III. Frameworks

Government needs to provide the frameworks to support the cybersecurity of our critical infrastructure, with incentives to drive the required behaviours and improvements. The Boards of each OES need to invest appropriately to manage the risks to critical systems and essential services. Ongoing effort from both the public and private sector is essential to keep up with changing threats and new technologies [4].

Public-private 'partnerships' are often described as being a 'cornerstone' of cybersecurity however clear lines of responsibility and accountability need to be defined as each side of the partnership has its own perspective. The private sector emphasises economic promotion and pays closest attention to the financial and reputational aspects of cybersecurity while the public sector retains responsibility for national security [5].

With most of critical infrastructure being privately owned, the combined provision of security by public and private actors requires a clearly defined arrangement [5]. The NIS Directive depends on OES knowing their own operating environments best and understanding the risks of their particular deployment of technology. The NIS Directive, being non-prescriptive, assumes OES are best placed to take appropriate steps to achieve the NIS outcomes against the backdrop of their risk appetite. Having a clear understanding of the risk appetite of the Board provides the context for how the NIS Directive is implemented [6]. This may or may not align with the government's perspective on national security as a public good.

The assumption that the private sector can invest in cybersecurity "beyond its cost/benefit analysis… to ensure national security" requires a clarity in oversight to achieve the required level of cybersecurity [5]. The supply chain oversight aspect of the NIS Directive in particular requires a substantial effort to assume responsibility for the cybersecurity of supply chain tiers.

Finding a way to measure the performance of cyber security work programmes is challenging. Forming quantitative measures of progress is taking time so there is a lack of data on the impact of the current National Cyber Security Programme [1]. There are questions around how to determine the relative contribution of each component of the strategy and how to assign values to the results of each component and to the overall outcomes, against the cost of the strategy [7]. Accountability must be clearly defined for measurement to be possible. Actions being measured need to be attributed to an individual or team or organisation i.e. it needs to be clear that their actions are the ones influencing the measured activity. "Performance measures should measure something that the organisation can reasonably be expected to influence" [8].

A common framework for performance measurement, that can be adopted by all relevant stakeholders, would enable better co-ordination and joined-up working across cybersecurity preparations and response [8]. The cross-government approach inherent in the Cyber Security Programme requires an overarching governance activity to maximise its effectiveness.

A review of National Security Capability in 2018 suggested ring-fencing cyber security within government department budgets to maintain it as a priority. This approach would require a coordinated strategy with "accountability for performance, risk and financial management" [1]. The

National Security capability review recommended improving accountability in a way that would shift incentives towards a more holistic approach across departments [9].

Forming the latest threat landscape requires multiple contributions and accountability. The Capability Review committed to ensuring the implementation of the National Cyber Security Strategy "keeps pace with the threat"[9]. This essentially requires continual re-assessment of the latest threats and making adjustments to the implementation where necessary to ensure activities are re-aligned with the latest risks.

A. NIS Scope & Beyond

The definitions of NIS relevant assets by each OES, to decide the scope for the CAF assessment, have included the supply chain to varying degrees. Figure 2 indicates the potential spheres of interaction with the NIS scope of assets and systems that essential services depend upon. In addition to external suppliers providing products and services that support the essential service, internal suppliers from enterprise spaces are interacting with the Operational Technology (OT) environment. There is also the continued malicious attempts to interact with critical networks and systems causing potential cyber incidents [10], [11].

IV. APPROACHES

Distinct approaches to NIS implementation by separate Competent Authorities overseeing different sectors are explored below following interviews and discussions with those sectors.

A. Competent Authority 1 (CA1)

This sector already had various regulations to meet before NIS came into effect. These were essentially safety focused. Both the OES and CA1 have separate teams dealing with safety and cyber security. The different safety specialisms are operating separately with some cyber security included. There is a move towards a more integrated approach between safety and cyber security with a long-term goal (4-5yrs) to have umbrella rules in place over cyber and safety together. Safety risks are meticulously documented, there is a side project ongoing by CA1 to apply cyber security to those risks [10], [12].

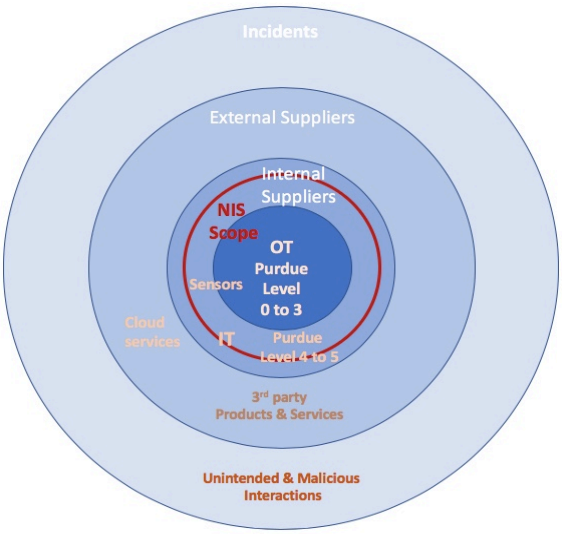

Figure 2 NIS Scoping Boundary

The scoping exercise CA1 have expected all OES to carry out, to identify NIS relevant assets, has brought together skillsets from right across OES organisations. IT and cybersecurity teams could not decide independently what was in scope, interactions with engineers, safety experts, operations etc. agreed the NIS scope for the whole organisation [12].

CA1 are using a matrix approach to assess the complexity of different facilities. They use this complexity level to decide which sites need auditing. They also decide how much time each should be given by auditors based on their latest performance review. On-going improvement and therefore the frequency of audits is also determined through this performance-based oversight. Some key suppliers to the industry are already in scope for audits due to being directly regulated under other regulations besides the NIS Directive [12].

CA1 have set up a framework to accredit cyber professionals to be auditors for their sector. The skillsets for accreditation have emphasised OT and ICS experience more than experience specific to the sector because the OESs already have that expertise so are more in need of cyber expertise for their audits and recommendations. In the longer term (2-3yrs) there could be potential for other sectors to tap into this network of cyber professionals including supply chains. This may also encourage some consistency across sectors [10], [12].

CA1 have pre-defined a profile to show expectations on the OES, what they expect to be achieved or partially achieved. Previous regulations they were working to used a prescriptive approach with yes or no type checklists. They prefer the outcome focused approach of the CAF for this context [12].

With regard to the notification of OES changes to CA1. While the safety cases are more intricate in the concept of change management, a simpler change process has been adopted for NIS. CA1 have given clear information on what changes need to be notified to them by OES, such as:

- Changes to the scope and the security boundary of critical assets (assets in scope of NIS).
- Change of supplier.
- Contact information [12].

Figure 3 presents a comparison of CA approaches to NIS.

	Competent Authority 1	Competent Authority 2	Competent Authority 3
Expectations on OES	CAF profile of NIS outcomes to be achieved.	Assess safety and cybersecurity risks together and take action to mitigate the highest risks.	Achieve a baseline capability defined in sector CAF.
Safety and cybersecurity	Separate safety and cyber teams. Gradual integration in longer term.	Integrated approach to safety and security.	Focus on cyber causing safety impacts to operational systems.
Planning inspections	Assess risk and complexity of facility & latest performance review.	Screening of self-assessments and improvement plans decides the priority for inspections.	Focus on cross-sector awareness raising and establishing baseline security requirements.
Auditors	Outsourcing audits through accreditation of cyber professionals with OT and ICS experience.	Building cybersecurity capability into existing regulatory role. Inspecting compliance level and setting actions to improve compliance.	Cybersecurity being integrated into existing inspectorate role.
Overseeing the changes	OES to notify changes in NIS scope or changes of supplier to CA.	Scope definition includes requirements of both safety and cybersecurity regulations.	Offering cybersecurity training to OT staff.
Supply Chain	Compiling list of suppliers and what is being supplied to OES. Responsibility is on OES to secure the supply chain aspect of their essential services.	Supply chains are one aspect of a considerable new implementation effort. OES must assure cybersecurity capability of organisations interacting with their NIS scope.	Awareness raising through supply chain briefings for whole sector.

Figure 3 Comparing CA Approaches to NIS

CA1 see a key advantage of the NIS Directive is that it has helped OES to gain Board support and therefore the required budgets and focused attention to meet NIS objectives. They have also received contact from smaller organisations that are not identified as OES but are interested in applying the CAF to their setting. This indicates there is interest and importance, beyond NIS implementation, to put resources into cyber security preparations [12].

At this point the supply chain is not directly in scope for NIS (other than through the responsibility on OES to secure their essential services including the supplier aspect to that). OESs are expected to provide a list of suppliers to CA1 and what they are supplying. OESs are responsible for managing their own risks. If they select a supplier with less security, for say lower costs, then they are expected to manage the risks associated with that decision [12], [13].

CA1 recognises a use for some measurement of supply chains that would show when a threshold is reached that indicates particular suppliers should be directly in scope of NIS. Some suppliers are already in scope under other regulations besides NIS. Some OES are passing on requirements to their supply chain and requesting supplier self-assessments [12], [13].

B. Competent Authority 2 (CA2)

Rather than adding a new cybersecurity and NIS team, CA2 is developing an integrated approach to safety and cybersecurity and building the cybersecurity capability from within their existing regulatory role. The definition of scope is inclusive of the requirements of both safety and cybersecurity regulations. Both safety and cyber security risks are assessed and the highest risks determine the actions and countermeasures taken [12].

CA2's existing audit and inspection activity includes cybersecurity as a potential cause of a safety incident. Sites that come under both safety regulations and the NIS Directive are being inspected against safety only, until a framework and training are in place by April 2020 to audit against NIS also. At this point, advice for NIS compliance is being given while enforcing safety regulations. Once the underlying systems and processes required to regulate against NIS are in place and training is complete, then the NIS enforcement activity will commence. Having both regulations in place will ensure a better coverage of issues at each facility. Direct causation of personal and environmental safety has so far been covered through safety regulations. The NIS implementation will ensure the indirect cyber causes of safety or environmental issues is added to the picture of risks [11].

Likewise, many of their OT sites are at the beginning of implementing security. The cybersecurity knowledge and implementations are growing steadily from within existing teams, with the OT teams gradually including new cybersecurity requirements. Supply chains are just one aspect of a considerable new work effort [10].

The self-assessments and improvement plans, being provided to CA2, provide a picture of different maturity levels and timescales of compliance across 70 sites, indicating in what areas better guidance is needed. Information is shared

with NCSC for guidance to be improved in weaker areas. The screening of the assessments and plans received from each site is used to decide which sites to prioritise with inspections. These inspections will aim to conclude how compliant a site actually is and set further actions, as required, to improve compliance [11].

Each individual site must define which network and information system zones are important to their essential services. Levels 0 through to 3 of the Purdue model [14] are regulated already for the prevention of safety incidents. The NIS sites also have infrastructure that live within IT at levels 4 and 5 of the Purdue model. Anything that interacts with these zones, with physical or logical access, the OES has security responsibility for under NIS. The OES therefore needs assurance of the competence of organisations interacting with their NIS scope. For example, if a data centre in another country is being used, Competent Authorities cannot regulate beyond their borders but the NIS Directive expects OES to be using appropriate levers and contractual arrangements to meet their security requirements. The legal duty sits with the NIS site in this context unless contracts are in place to effectively share responsibilities [10]. CA2 will assess:

- Evidence that a supplier is fit for purpose.
- If reasonable measures are being taken by the NIS site to communicate and enforce security requirements.
- If the NIS site is taking a proportionate approach to meeting essential requirements, eg if processes are in place for bringing hardware onto site, or for secure remote software changes etc [11].

C. *Competent Authority 3 (CA3)*

Competent Authorities, with guidance from the NCSC, are setting expectations on the OES in their sector by defining a CAF profile to achieve. CA3's approach to this demonstrates the initial focus of NIS implementation has been about achieving a baseline capability. Their emphasis is currently on what is achievable rather than using a more risk-based approach to decide what is important. While the NIS Directive is aiming towards a level of cyber resilience towards well-resourced and capable adversaries, CA3 have set an initial target to achieve a baseline profile, aiming at a level more appropriate for limited capability. This stage is essentially about awareness raising and establishing a baseline [10], [12].

Moving to a higher level of cybersecurity capability will require a closer analysis of risks to this sector, to emphasise the elements of the CAF that have the most influence on reducing those risks. A framework for performance measurement would enable the monitoring of progress, drive improvements and facilitate needed interventions.

V. Broader Frameworks of Assurance

Aside from the NIS Directive, the NCSC provide general Supply Chain Guidance which holds similar expectations of supply chain visibility and the achievement of an appropriate level of control [15]. The NIS Directive itself has focused on assessing individual OES and requires our dependence on international supply chains to be met by "appropriate and proportionate" measures taken by OES to secure them. While there is a reliance on third parties, it is expected that the responsibility for protecting the essential service remains with the OES [2]. Despite the Supply Chain Guidance offered and the requirements of the NIS Directive, a more "robust supply-chain framework for cybersecurity" is needed to assist this accountability [16]. This implies a broader oversight of activities is required than the individual responses of OES. The intention of such a framework would be to:

- Assess the broader impact of NIS on the resilience of essential services.
- Widen cyber maturity assessment to consider dependencies across supply chains.
- Inform interventions by accountable parties.
- Provide cross-sector insights.
- Improve oversight and governance activity within and across sectors.

A. *NCSC Supply Chain Guidance*

The guidance coming from NCSC outlines four key stages to supply chain security [15]:

1. Understand the risks
2. Establish Control
3. Check your arrangements
4. Continuous improvement.

The first stage of understanding risk essentially should expand into managing those risks. Establishing an achievable level of control involves defining and agreeing supply chain involvement in the cybersecurity process of protection, detection, response and recovery. Checking agreements and contractual arrangements requires a regular assessment of suppliers' contributions to cybersecurity capability. Achieving a cycle of continuous improvement would be aided by managing dependencies on suppliers to achieve the required improvements.

Figure 4 demonstrates some of the activities required in each of these four stages and indicates that continuous checking of supply chain arrangements will require a performance monitoring activity in order to identify interventions and improvements where most needed.

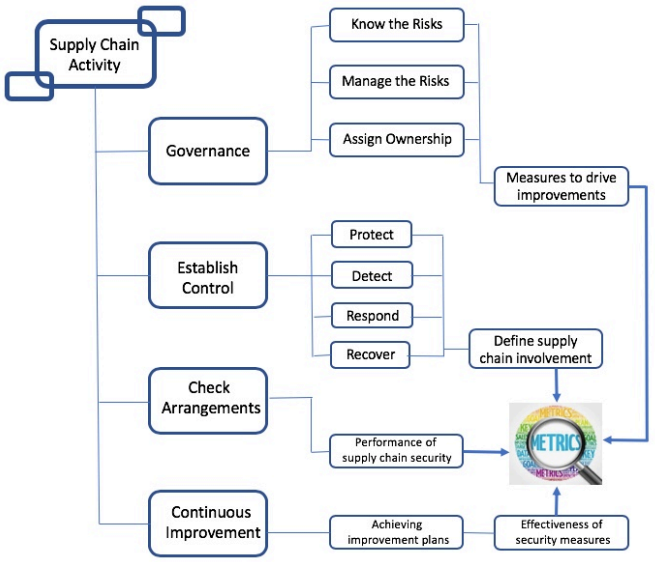

Figure 4 Supply Chain Activity

The information gathering activity in 'Understand the risks' must be ongoing and linked to 'Continuous Improvement' hence it has been described here as a Governance activity that includes agreeing accountability and assigning ownership of the risks.

The following chart in Figure 5 expands further this Governance activity. In order to 'Know the Risks' OES are including cyber security assessments in their procurement processes to understand the risks presented by each new supplier. This is enabling a level of importance to an OES's essential service to be assigned to each supplier and a corresponding response in terms of assuring a suppliers' compliance with security requirements. The level of oversight of suppliers is prioritised according to their involvement in providing and supporting critical assets and services within the scope of NIS. Achieving this with existing suppliers as contracts are renewed to include cybersecurity requirements is a more gradual, long term process.

The return of procurement questionnaires by amenable suppliers is providing a partial picture but is a long way off the more complete visibility required to really 'Know the Risks' [10][13][17]. Individual security questionnaires coming from each customer are causing a considerable overhead for suppliers. With a fair proportion of this activity covering common ground, this points to potential for developing common methods and improving efficiencies in security assurance. For a more effective accountability, roles and responsibilities and achievable goals need to be clearly articulated with a consensus on the value of the defined approach [18]. The value-add in procurement processes could be improved upon through better analysis of responses to the question set and sufficient follow up to ensure requirements are met [6].

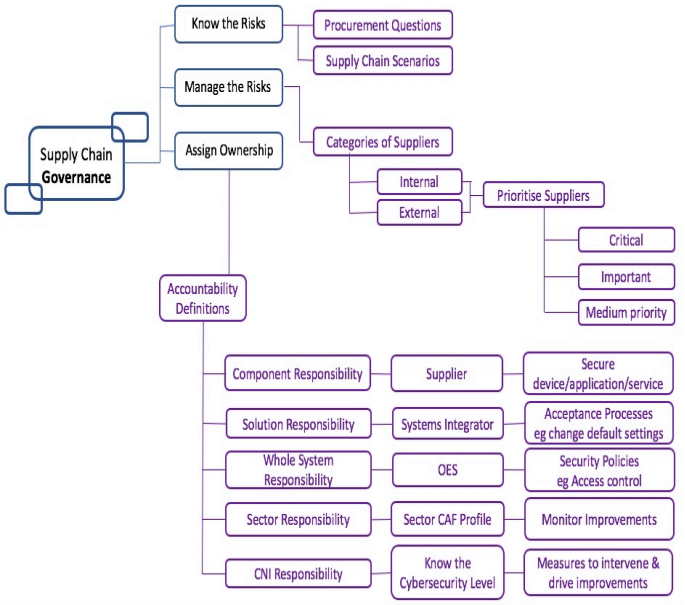

Figure 5 Supply Chain Governance

Guidance on potential attack scenarios to prepare for would also assist in focusing activity towards evolving threats. The NIS Directive expects OES to know and understand their risks and the threats to their sector. However, the uncertainty in this area has been consistent. This is where government can offer a meaningful contribution through assisting OES to form a clearer threat picture [19].

The NIS Directive has been formulated in a way that assumes OES to have a hierarchical control over their supply chains and the CAF expects a deep understanding of the supply chain [20]. The process of implementing NIS is presenting areas of their supply chains where OES have less negotiating power, or a lack of choice in suppliers, to influence the required level of cybersecurity. Tiers of the supply chain are not managed or understood. A very limited visibility of sub-contractors is common. Longstanding contracts often do not include cybersecurity requirements and legacy equipment lacks the capability to provide security [10], [13].

Oversight by CAs is looking for shared responsibility models to be agreed with suppliers [20]. The standard IEC62443 on security for industrial automation and control systems is made up of component, system, policies and overview levels [21]. Responsibility for the security at each of those levels needs to be assigned appropriately, as suggested by the accountability definitions in Figure 5.

Self organising networks have developed to work together on these issues. One sector has taken this approach through a committee of several OES meeting with critical suppliers one by one to discuss their common security requirements [6]. This can succeed as far as the significance of their shared common denominator. This OES network would also prefer to

be able to meet with suppliers as a group to develop some consistency and new norms with their key security requirements [6]. There is potential for governments to do more with coordinating and motivating these self-regulating networks [19]. The current ad hoc approach, while all the risk in the supply chain is held by the buyer, needs a clear mechanism to be developed that can accommodate the dynamic property of this situation such that changes or new vulnerabilities in the supply chain, that are likely to impact with high consequences, can be flagged appropriately [6].

While the NIS Directive is being adopted by individual OES to varying degrees, the actual contributors to their overall cybersecurity level comes from a broader set of organisations. Systems integrators are not always receiving appropriate direction or guidance in terms of clearly defined acceptance processes or end to end system security requirements [17]. Beyond knowing the risks and the current cyber security capability is an ongoing activity that requires governance and oversight to manage the:

- Contributions to reducing the attack surface.
- Contributions to understanding the latest threat landscape.
- Contributions to minimising the impact of incidents.

Otherwise decisions will continue to be made in isolation or without reference to clear security requirements or a full risk picture.

VI. Proposed Framework

This section proposes a framework to demonstrate a "discipline of complex interdependency" and to guide cooperative and reciprocal adjustments by all relevant parties [22]. Instead of establishing control by securing component levels and aggregating this into achievement of the strategic NIS outcomes, there are multiple influences towards reaching the requirements of the NIS Directive. Going beyond a focus on the responsibility of individual OESs to secure their essential service, Figure 6 presents a combination of elements and interactions that all contribute towards achieving a secure essential service. By taking a cross-section of individual and collective contributions, it shows four different views to cover the diverse influences affecting the cybersecurity level achieved.

In the Component quadrant, it considers the component parts, the devices and people, that make up the OT solution and processes, such as assurance from suppliers on the security of their equipment. It includes behaviours at an individual level, including cyber awareness of employees, managing contractors and considers insider threats.

The OT quadrant considers the behaviour that emerges from the interaction of components, such as the interaction of OT areas with enterprise systems or remote support from

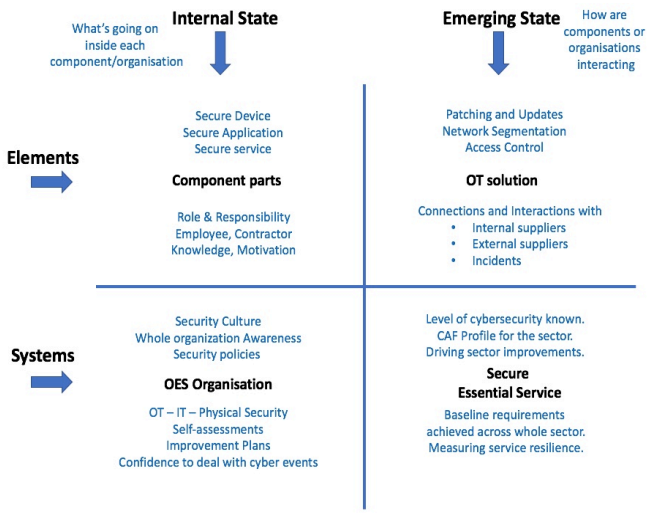

Figure 6 Securing Elements & Systems

external suppliers and interactions with potential incidents or attack scenarios.

The OES quadrant considers the security culture of an OES organisation and awareness across the whole organisation building the confidence to deal with cyber events. This quadrant also shows what is achievable for an OES within their cost/benefit model and with the information, motivation and cooperation available to their single organisation.

The Essential Service quadrant assesses the holistic cybersecurity for the particular service This is where the CAF profile for the sector is decided, setting achievable aims to drive sector improvements, and where dependencies across the whole sector to achieve an agreed cybersecurity level are understood. This quadrant is where a view of the shared responsibility model appears from what is being achieved and not achieved through NIS.

The performance of this multi-faceted activity could be monitored by selecting metrics that ensure each of the quadrants in Figure 6 is engaged efficiently and effectively and contributing to the principles of the NIS Directive.

Figure 7 offers another example of taking a cross section of internal and emerging states, considering the elements and systems involved, for the NIS implementation itself. The first quadrant looks at the progress within each NIS Scope per OES, with each NIS scope being an element of improvement for the sector.

The Levers & Contracts quadrant goes beyond the NIS boundaries and scopes to investigate the broader influence from supply chain organisations. It looks at the gradual process of establishing supplier contracts with security requirements and the effectiveness of influences on the supply chain. The potential for cybersecurity being integrated as standard in supplier offerings is also considered here.

The industry sector quadrant considers a particular sector as a whole. It includes risk assessments by the CA to decide where to focus resources and which OESs to audit. It also sees the dependencies involved to reach a particular target cybersecurity level for the sector. It defines the response coming from the CA with improved guidance or support for weaker areas.

The Critical Infrastructure quadrant contains a more strategic oversight, considering the interdependent relationships and the risks to essential functions that cannot be managed or controlled by the responsible OES. It offers the potential to develop more consistency across different sectors. This quadrant aims to building an overall picture of cybersecurity capability across each sector and enable decisions and interventions to improve the resilience of critical infrastructure. It is important to understand the differing levels of capability from various actors and see how this is impacting the resilience of essential services.

Figure 7 describes the high-level engagement activity required to compile a more complete picture and effectively monitor progress. A selection of appropriate metrics would assess the contribution of each of these four areas towards improving cybersecurity and resilience of critical national infrastructure. Incentives and resources must be in place to sustain the accountability of actors and achieve the agreed goals and responsibilities. Evaluation mechanisms are needed to assess if objectives have been met and to demonstrate the impact of the Directive [23]. For example, in the telecoms sector, governments have been exploring how to incentivise operators to prioritise the cybersecurity of 5G networks, with the EU proposing a toolbox of measures to guide member states in securing their networks [24].

Managing cybersecurity risks essentially requires the ability to identify a change in security risks and to make an informed response to that change. There are multiple levels to this activity. Achievement of the CAF requires an approach to supply chain risk management that prepares essential functions for "subversion by capable and well-resourced attackers" [20]. This level of cybersecurity is currently unachievable by OES working independently and assessed as individual organisations. Fostering assurance collaborations with a consistent approach to managing risks across organisations and supply chains would aid this effort.

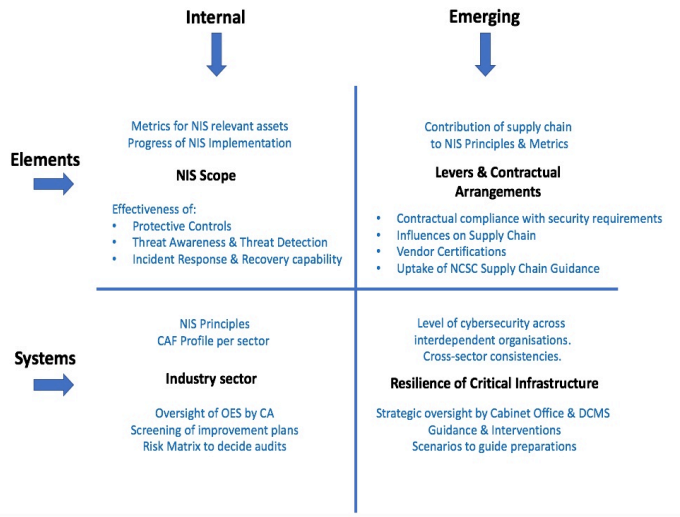

Figure 7 Broader Impact of the NIS Directive

VII. Interdependent Assurance

This section outlines some key activities across private organisations and government departments that all contribute to the assurance of essential services. Paying attention to performance and achievement in these areas would begin the more 'robust performance framework' requested by the National Audit Office [1].

Table 1 pays attention to some of the contributing elements of an essential service, including relations with and assurance from vendors and individual human factors. Table 2 outlines some key activities to secure NIS critical assets including OES engagement with vendors and systems integrators.

Table 1 Supplier and human factor assurance activities

Components, People and Products
Technical product assurance from suppliers. - Cyber security integrated into supplier offering, rather than being a chargeable extra. - Patching security vulnerabilities through lifecycle of product.
Management of tiers within supply chain - Assurance of tier 1 suppliers risk management processes with their suppliers. - Security requirements specified in supplier contracts. - Notification to OES of decision to sub-contract.
Individual Behaviours - Cyber skills and awareness of employees and contractors. Policies in place to reduce risks of insider threats.
Collaborations (legal contracts cannot contain/manage the whole problem) - Establish workgroups, operators and key suppliers working together on improvements to cybersecurity. - Key supplier involvement in cyber exercises with operators.

Table 2 Assurance of NIS critical assets

OT solutions. Assurance of NIS Scope
Assessing Process & System Resilience - Number of vulnerabilities in processes and systems and security controls. - Outstanding workload to secure, number of vulnerabilities unpatched. - Decide priorities, consider exposure to threats and potential impact. - Preparations in place for a set of scenarios. - Incident response practices with suppliers. - OT Security requirements communicated to systems integrators to guide their implementations.

Table 3 describes assurance actions within an individual OES organisation including building a security culture, a complete set of security policies and the management and treatment of risks. Table 4 considers the assurance activities for a whole industry sector including regulatory and guidance activities of the CA and the approach to managing risks across the sector. Table 5 outlines the strategic level of assurance through cyber resilience assessments of national critical infrastructure. This would aim for consistent approaches across sectors and ensure activities are keeping pace with the latest threats.

Table 3 Assurance of OES organisation

OES Assurance of Essential Service **Security Culture & Awareness**
Process of NIS Implementation - Monitoring improvements. - Measure of organisation's security culture. - Level of confidence to protect & respond.
Security policies, procedures & guidelines - Are thorough and complete & updated regularly. - Approved by management & assigned to committed owners.
OES Risk Appetite - Is clearly defined & formally documented. - Security risks are Identified, Analysed & Quantified.
Risk Register - Is in place & fully complete. - Updated regularly & under regular review. - Identifies risk levels as high/med/low. - Shows number of risks currently untreated or unresolved.
Treatment of risks - Risks are reviewed and audited regularly. - Brought within defined risk tolerance levels.
Variations in security budget - Reflecting the ability to achieve or maintain a security level. - Indicating a change in risk appetite.

Table 4 Whole sector assurance activity

Industry Sector
CA Risk Process - Risk assessments to decide audits. - Response to CAF returns with improved guidance & support for specifics.
Consistency of risk management - Comparison of cyber security risk management processes across vendors, OES, CA.

Table 5 Critical Infrastructure Assurance

Resilience of Critical Infrastructure
Cyber Resilience Assessment - Availability of Essential Services. - Cybersecurity Capability level. - Consistent behaviours of People & Systems. - Evolving threat landscape, scenarios to guide preparations are communicated. - Shared responsibility is agreed for risks that are unmanageable by individual OES. - Cyber security solutions enabling new technology and new services to be launched securely.

The regulatory activity underpinning the cybersecurity of our essential services is dynamic, with multiple actors participating. It requires coordination across a distributed accountability and effective communication across actors to improve their capacity to make more informed decisions while protecting our infrastructure and responding to events [25].

VIII. International Cooperation

The National Security Capability Review supported extending our operational reach through continued international cooperation with ENISA and Europol, especially to continue sharing information, furthering industry collaborations and to reduce the potential attack surface [9]. There is therefore a further activity to form ongoing relations with and contributions to the NIS Cooperation Group, where consistency of NIS Implementations across participating countries is encouraged. Outcomes of our NIS Implementations could be fed back into the Cooperation Group to evaluate the broader resilience envisaged by NIS.

IX. Future Work

A set of metrics to enable the oversight activity described here and evaluate the effectiveness of national cybersecurity policy is currently being developed, alongside engagement with several industry sectors. Clarity on roles and responsibilities between the public and private sector is essential to take this forward. Developing a set of metrics to oversee and drive this broader activity will establish baselines to measure progress against and enable high level and specific priorities to be decided. The metrics will aim to indicate both the longer term and short-term activities required for an adaptive Cyber Security Programme, such as long-term skill and knowledge development alongside the short-term response to evolving threats and changing risks.

ACKNOWLEDGMENTS

This project is overseen by RITICS, funded by NCSC and EPSRC. Acknowledgement goes to several OES and CA from different NIS industry sectors for providing useful input to this project.

REFERENCES

[1] National Audit Office, 'Progress of the 2016 – 2021 National Cyber Security Programme Key facts', 2019.

[2] 'NIS Guidance Collection', 2018.

[3] NCSC, 'The NCSC Annual Review 2019', 2020.

[4] Cabinet Office, 'National Cyber Security Strategy 2016 - 2021 | Progress Report', 2019.

[5] M. Carr, 'Public-private partnerships in national cyber-security strategies', *Int. Aff.*, vol. 92, no. 1, 2016.

[6] 'Author's interviews with industry', 2020.

[7] National Audit Office, 'The UK cyber security strategy: Landscape review', 2013.

[8] HM Treasury, Cabinet Office, National Audit Office, Audit Commission, and Office For National Statistics, 'Choosing the Right FABRIC', 2001.

[9] HM Government, 'National Security Capability Review – March 2018', no. March, p. 49, 2018.

[10] T. Wallis, 'Author's interviews with OES', 2019.

[11] T. Wallis, 'Author's interviews with CA', 2020.

[12] T. Wallis, 'Author's interviews with CA', 2019.

[13] T. Wallis, 'Author's interviews with OES', 2020.

[14] H. Li and T. Williams, 'Some extensions to the Purdue Enterprise Reference Architecture (PERA)', *Comput. Ind.*, vol. 34, pp. 247–259, Dec. 1997.

[15] NCSC, 'The principles of supply chain security'. [Online]. Available: https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security.

[16] M. Shukla, S. D. Johnson, and P. Jones, 'Does the NIS implementation strategy effectively address cyber security risks in the UK?', *2019 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2019*, pp. 1–11, 2019.

[17] T. Wallis, 'Author's interviews with suppliers to OES', 2020.

[18] P. Vaillancourt Rosenau, 'The Strengths and Weaknesses of Public-Private Policy Partnerships', *Am. Behav. Sci.*, vol. 43, no. 1, pp. 10–34.

[19] M. Dunn-Cavelty and M. Suter, 'Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection', *Int. J. Crit. Infrastruct. Prot.*, vol. 2, no. 4, pp. 179–187, 2009.

[20] National Cyber Security Centre, 'The Cyber Assessment Framework (CAF)', no. September, 2019.

[21] ISA, 'ISA Standards'. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-in-numerical-order/.

[22] J. Braithwaite and P. Drahos, *Global Business Regulation*. Cambridge University Press, 2000.

[23] J. Stiglitz and S. Wallsten, 'Public-Private Technology Partnerships', *Am. Behav. Sci.*, vol. 43, no. 1, pp. 52–73, 1999.

[24] J. Sullivan and R. Lucas, '5G Cyber Security A Risk-Management Approach', *Glob. Technol. RUSI Occas. Pap.*, vol. February, 2020.

[25] R. Baldwin, M. Cave, and M. Lodge, *Understanding Regulation: Theory, Strategy and Practice*. Oxford University Press, 2012.