Information & Security

T. Wallis, C. Johnson & M. Khamis
vol. 48, no. 1 (2021): 36-68
https://doi.org/10.11610/isij.4812

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Interorganizational Cooperation in Supply Chain Cybersecurity: A Cross-Industry Study of the Effectiveness of the UK Implementation of the NIS Directive

Tania Wallis [1] (✉), *Chris Johnson* [2], *Mohamed Khamis* [1]

[1] *University of Glasgow, Scotland, UK, http://www.gla.ac.uk*

[2] *Queens University Belfast, Northern Ireland, http://www.qub.ac.uk*

ABSTRACT:

The transposition of the EU Directive on Network and Information Security (NIS) by EU Member States involved assigning a set of responsibilities to operators, regulators and policy makers within a national cybersecurity strategy, in order to improve cybersecurity levels across critical infrastructures. This research investigates the perspectives and experiences of organisations affected by the NIS Directive focussing on three different sectors (Energy, Water & Aviation). The authors evaluate the response of different actors to NIS interventions and their challenges in meeting their assigned responsibilities, in particular their ability to oversee supply chain cybersecurity. It proposes further support for partnerships and cooperation across organisations to increase the effectiveness of NIS implementation. Based on results from semi-structured interviews and observations of industry working groups, an approach to supply chain oversight to achieve a balance between control and cooperation is recommended, to improve cybersecurity within industry sectors and across critical national infrastructures. Although our initial focus has been on working mainly with UK stakeholders, we argue that our recommendations have a more general application beyond those countries directly affected by the Directive.

ARTICLE INFO:

RECEIVED: 29 APR 2021
REVISED: 06 MAY 2021
ONLINE: 08 MAY 2021

KEYWORDS:

cybersecurity, critical infrastructure, essential services, supply chain, operational technology, interorganizational cooperation

✉ E-mail: tania.wallis@glasgow.ac.uk

1. Introduction

1.1 Regulation of Critical Infrastructure

The EU Directive on Security of Network and Information Systems (NIS Directive) was introduced in 2016 to raise the cybersecurity level of Critical National Infrastructures (CNI) across EU Member States.[1] A reform of the Directive was proposed by the European Commission in December 2020 known as NIS2.0.[2] The original objectives of the NIS Directive are still considered as very relevant:

- to increase the capabilities of Member States in mitigating cybersecurity risks and handling incidents
- to improve the level of cooperation amongst Member States in cybersecurity and the protection of essential services
- to promote a culture of cybersecurity across all sectors vital for our economy and society.

It applies to industries providing essential services to society such as Energy, Water, Transport, Health and Finance. The interpretation of which companies fall within scope across these industries is a matter for individual member states. The NIS Directive places a responsibility on national Governments to secure their essential services. The transposition of the NIS Directive by each national Government decides the services considered essential for their nation and applies the regulation to the public or private operators of those services.

It was transposed into UK law in 2018 as the *NIS Regulations*. These regulations are still in place following the UK's departure from the European Union and will be reviewed by the UK Government during 2021.The UK National Cyber Security Centre (NCSC) produced a collection of guidance for the implementation of the UK NIS Regulations. Figure 1 outlines the principles and objectives that are defined in the NIS Guidance Collection.[3] This paper evaluates the response of different actors to these NIS Objectives & Principles and their challenges in meeting this intervention.

The original NIS principles are further outlined in Table 1; this provides an overview of what is expected of each operator of essential services as defined under the NIS Regulations. The NIS Directive introduced key roles and responsibilities as listed in Table 2.

The NIS Directive expects national Governments to have a National Cybersecurity Strategy with the goal of improving the cybersecurity level of their critical infrastructure and securing the services essential to their society. Figure 2 shows how the UK's implementation of this high-level strategy engaged organisations and activities across the public and private sector and demonstrates the full extent of the supply chain being positioned within OES responsibilities. This supply chain includes the hardware, software and systems being used by operators to provide their essential services such as water or electricity supply or transport services. It can include systems integrators who are configuring bespoke designs; providers carrying out maintenance for an operational facility or

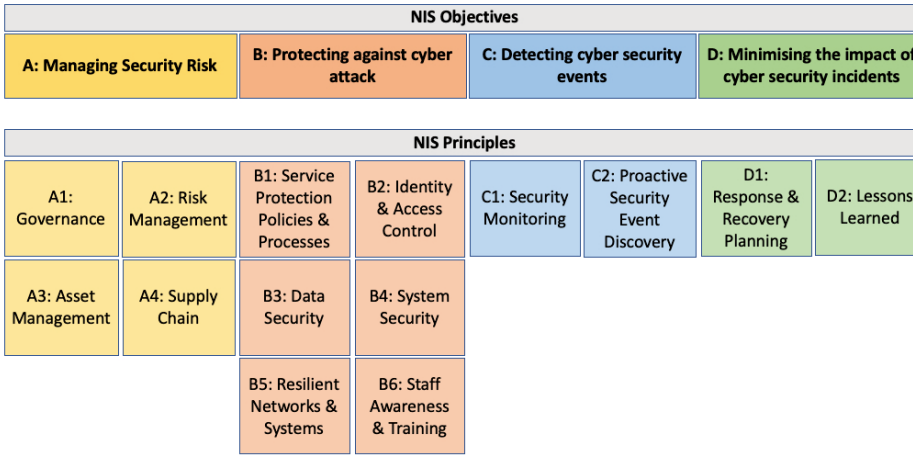

Figure 1: NIS Objectives & Principles.[4]

support services for IT or Operational Technology (OT). The supply chain could also include consultants providing relevant expertise to an OES. It is up to the OES to decide what is in scope of the NIS Regulation by defining the critical assets and suppliers that their essential service is dependent upon.

The UK National Cyber Security Centre (NCSC) provides overall guidance by producing indicators of good practice that contribute to the outcomes expected by the NIS principles and objectives.[5] The sectoral Competent Authority (CA)

Table 1. NIS principles.[6]

Objective A	Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to essential services.
Objective B	Proportionate security measures in place to protect essential services and systems from cyber-attack. Includes: identity and access control, data and service security, information protection policies and processes, protective technology and staff awareness and training.
Objective C	Capabilities to ensure security defences remain effective and to detect cybersecurity events affecting, or with the potential to affect, essential services. Includes security monitoring and anomaly detection.
Objective D	Capabilities to minimise the impacts of a cyber security incident on the delivery of essential services including the restoration of those services where necessary. Includes response and recovery plans.

Table 2. Roles & Responsibilities introduced by the NIS Directive.[7]

Role	Responsibility
Operators of Essential Services (OES)	Implementing NIS Principles. Required to report incidents affecting essential services to the Competent Authority.
Competent Authorities (CA)	Produce guidance & cybersecurity assurance goals. Audit and assess the cybersecurity levels achieved by OES. Enforce compliance where necessary.
Computer Security Incident Response Teams (CSIRT)	Provide technical expertise. Assistance with cybersecurity incidents.
Single Point of Contact (SPOC)	International co-operation and engagement with EU partners. Participation in the NIS Cooperation Group.

provides sector specific guidelines and a profile to be achieved that their assessments and audits are based on. In most cases, the nominated CA was the regulator in charge of existing safety oversight. Examples of organisations assigned the role of CA under NIS include the Civil Aviation Authority (CAA), Health & Safety Executive (HSE), and the Drinking Water Inspectorate (DWI). There is a reliance on OES to relate this to their specific operational context by defining the assets in scope of NIS that their essential service depends upon, assessing their current achievement against the provided Cyber Assessment Framework[8] and creating performance improvement plans that are overseen by the sectoral CA. While this process displayed in Figure 2 implies a passing of responsibility from the strategic level down to achievement of the goals of the NIS Regulations, our research demonstrates that collaborations and regular interactions are required between the private and public organisations involved to manage progress and provide assistance.

1.2 Managing Supply Chain Risks

The increasing digitalisation of CNI together with a need for more distributed forms of control, for instance as a consequence of the pandemic, has increased the need for more enhanced supply chain assurance. With many distributed devices and interactions over a mix of infrastructures, establishing a common level of mutual trust and security across different administration boundaries becomes increasingly important. Reliance on multiple vendors including open-source providers requires a closer understanding of the varying levels of their security so that the context of operational dependencies can inform ongoing improvements. Cyber criminals look for the weakest link where there are fewer protections in place because a single compromise in the supply chain can enable

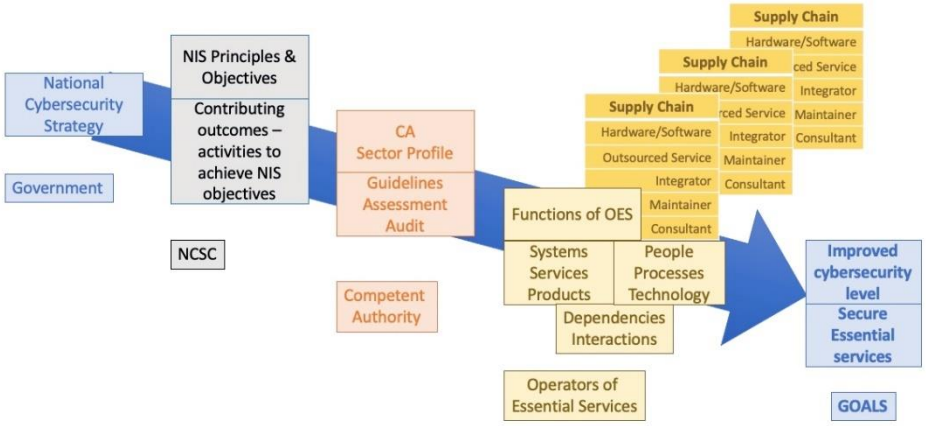

Figure 2: Implementing the National Cybersecurity Strategy for Critical Infrastructure.

access to multiple organisations. A significant proportion of attacks are targeting beyond one organisation and intending to achieve access to other organisations along their supply chain.[9] Increasingly the vendors and suppliers used extend across national borders raising significant concerns about national security and "digital sovereignty."

The NIS regulations do not directly apply to the supply chain. Instead, there is a pass down of responsibility where operators need support from their vendors to achieve adequate cybersecurity and reduce risks to their infrastructure. NIS Objective A and principle 4 in the Cyber Assessment Framework requires some oversight of OES supply chains. Table 3 shows some of the expected outcomes to fully achieve this supply chain principle. It requires operators to have a deep and broad understanding of their supply chain risks beyond Tier 1 suppliers and to have clearly defined supplier responsibilities as well as achieve a mutual commitment from suppliers to resolving incidents.[10]

This research, on examining the process of implementing the NIS Directive, highlights that OES, as individual organisations, are not in a position to fully secure their infrastructure and services without reaching out in collaboration with other organisations to develop sector approaches and to influence improvements in their supply chains. This creates a potential role for the CAs and wider government agencies in supporting collaborative approaches to supply chain assurance across national industries. There are tensions where this might be interpreted as undue interference in market forces; for instance, if a government agency forced OES to procure key components from an approved supplier list.

Table 3. Achieving NIS Principle A4a Supply Chain.

Expected outcomes to fully achieve NIS Principle on Supply Chains
Deep understanding of supply chain, including sub-contractors and wider risks, to inform risk assessment and procurement processes.
Consider risks to essential functions arising from supply chain subversion by capable and well-resources attackers.
Information shared with suppliers, that is essential to operation, is appropriately protected from sophisticated attacks.
Security requirements of suppliers are mutually understood and laid in contracts, with a clear and documented shared-responsibility model.
All network connections and data sharing with third parties is managed effectively and proportionately.
Incident management processes include mutual support with suppliers for the resolution of incidents.

1.3 Supply Chain Compromises

Recent supply chain attacks demonstrate that suppliers are a potential attack route into multiple operators. By compromising one vendor an attacker could achieve access to all the vendor's customers. Operators can also be caught in the crossfire of attacks targeted elsewhere due to sharing common vulnerabilities. The inability of suppliers to maintain adequate security over the long lifespan that equipment is used in cyber-physical systems exacerbates the situation. There can be several steps to an attack, once access is achieved, the attacker could move laterally within the network and reach more critical assets, such as operational technologies that control critical infrastructure. Layers of security, including segmentation of networks, are essential to minimise the impact of incidents. Urciuoli et al. present examples of supply chain threats to emphasise the importance of protecting the supply chain information layer.[11] Pandey and Singh describe a range of methods of attacking supply chain systems, from pre-installed malware on manufacturer components, to Denial of Service (DoS) attacks compromising availability of resources, direct attacks to damage and destroy services and, in particular, the ease of initial attacks against a third-party enabling access to their ultimate target.[12]

A global supply chain survey by BlueVoyant reported that 80 % of participants had experienced a third-party breach during the past year and 77 % have limited visibility of their supply chain, with only 2 % managing to monitor their vendors in real time or daily. The energy system is becoming more distributed with an increasing reliance on third parties. Distributed DoS is a key concern for the energy sector as well as third-party compromise of their SCADA systems.[13]

The continued obligation on OES to maintain their essential services has resulted in them being ideal targets for disruptive attacks such as ransomware.

Such attacks block access to important data until a ransom is paid and create an urgency to pay with threats to publish the stolen private and confidential information within a short timeframe. Several energy firms experienced ransomware attacks in 2020 such as the Ragnar Locker ransomware impacting Portugal's energy operator EDP, which targeted software used by their Managed Service Providers.[14] The Netwalker ransomware affected K Electric in Pakistan and multinational energy company Enel.[15]

Attacks in the water sector have resulted in a diverse set of impacts such as polluting water ways, data breaches and theft of irrigation water.[16] The water sector is dependent on the supply chain for essential chemicals for water treatment and therefore could be impacted by unauthorised intrusion into the ordering systems of their suppliers. A recent attack on a water treatment facility in Florida attempted to manipulate chemical levels in the water by adjusting set points. This attack emphasised the importance of maintaining integrity of system configurations, managing remote access to operational facilities as well as the human aspect, the anomaly in operational settings was discovered and corrected by a human operator.[17]

The aviation sector has experienced DoS attacks on air traffic communication channels and malware being introduced by sub-contractors into air traffic management systems. Airports already give much attention to physical security and require equivalent attention to cybersecurity, such as controlling digital access to their operational equipment.[18] Also, recovering safely from incidents is essential and requires close coordination with IT service providers to ensure safe operations are preserved during incident response and recovery.[19]

Aviation companies, along with other critical sectors, were alerted to consider their supply chains during the SolarWinds cyber-attack in 2020, which enabled the theft of FireEye's 'red team' tools that are used to test client defences by emulating adversaries. The attack also targeted the US Federal Government and the US Military and was achieved through a malicious software update by deploying malware as an update from SolarWinds' own servers. It was digitally signed by a valid digital certificate bearing their name. When customers updated the software, a backdoor was installed into their server. Its impact goes far beyond the original targets, after being unknowingly installed by IT administrators across 18,000 or more organisations. It has also left uncertainties due to the exposure of backdoors enabling additional exploits before discovery and patching was carried out.[20]

Microsoft exchange servers have recently been attacked globally by utilising four different vulnerabilities to gain high privileged access to the servers, prior to authentication and without valid credentials. Attackers could use this as a stepping-stone to reach other parts of the breached network, giving the opportunity for further exploits such as data theft or installation of malware. This attack demonstrates the importance of having an up-to-date asset inventory to find the affected systems quickly and take remedial actions. There can be a time lag before patching is possible, especially in operational environments, where it

is important to first assess if the patch would have a negative impact on system operation.[21]

The theft of customer records from credit reporting agency Equifax in 2017 was achieved due to an open-source software vulnerability. The lessons from the Equifax incident showed that implementation and management of security is just as important as having security procedures in place. Procedures were in place but the software vulnerability had not been patched. There was no network segmentation configured, attackers were able to go from machine to machine. Role based access control was also not set up, the system gave access to all the content once compromised. Anomaly detection for unusual behaviour was also not installed, thousands of database queries in rapid sequence was not alerted. Despite Equifax having a high spend on security, the actual implementation of it was inadequate.[22] Breaches related to open-source components have reduced since the Equifax incident but are still occurring often. In Sonatype's survey of software developers 20 % experienced a breach in 2020 that was tied to an open-source component.[23] Attackers are also not limited to exploiting the existing vulnerabilities within open-source components. Malicious actors now proactively target open-source projects by newly infecting software components to distribute malware.[24]

The cost of cybercrime to UK businesses is estimated to be £ 21 billion per year [25] and the average cost of cybercrime to an organisation is £ 8 million.[26] The time taken to deal with breaches is a significant issue while staff are prevented from carrying out their normal duties.[27] In addition to the operational recovery effort, company reputations and stock prices are also impacted.

2. Related Work

Sobb & Turnbull point out the need for additional research on evaluating the risks introduced from supply chains into operational environments and how to securely integrate supply chain technologies into such contexts.[28]

Other research methods have provided supply chain attack surface diagrams to assist with identifying gaps in current practices;[29] have modelled threat scenarios and potential attacks coming from a supply chain perspective;[30] and adapted attack graph generation methods to a dynamic supply chain environment to assist administrators with protecting assets.[31]

The international standard IEC62443 describes various aspects of industrial cybersecurity, including IEC62443-2-4 which specifies the security capabilities required of providers to industrial control systems.[32] ENISA provide good practices for cybersecurity across the supply chain for Internet of Things (IoT).[33]

Previous research has recognised that a single entity alone does not possess the full capability to respond to cyber threats without some level of cooperation with other entities. Polischuk recommends to focus and multiply the necessary capability through a flexible and adaptive national security system with effective communication between the elements of this system.[34]

Penchev and Shalamanova propose to establish focus groups under an umbrella organisation for the necessary cooperation between civilian and military

organisations in cybersecurity.[35] Other work exemplifies building an integrated collaborative information environment for more effective working across organisations during crisis management and to support decision making at different levels of Government.[36] This research provides a synthesis of this necessity for interorganisational cooperation in cybersecurity with other related works on the performance and resilience of supply chains, from supply chain management literature that are outlined in Section **Error! Reference source not found.**.

This article evaluates the experiences of implementing the NIS Directive across the public and private sector. It presents recommendations on supplier assurance and offers a timely contribution as the EU proposes to broaden the application of the NIS Directive and bring supply chains under the NIS umbrella. NIS regulated entities who deliver essential services in the EU will be required to "assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures."[37]

3. Research Method

This research included interviews with organisations in the Energy, Water and Transport sectors. The experiences of each of the roles and responsibilities supporting the implementation of the NIS Directive were included. This enabled the challenges to be understood from the different perspectives of providers of essential services, their suppliers and regulators. Due to the sensitivity of the topic and to investigate different approaches being used and identify the barriers to progress, semi-structured interviews and discussions captured the different viewpoints. The lead author also participated in industry collaborations and working groups that were formulated to progress the supply chain resilience effort and to review the progress of the NIS Directive. This assisted in building trust with interviewees due to the sensitive nature of cybersecurity. This paper is based on semi-structured interviews and observations of industry working groups. The names of organisations and participants are not disclosed for confidentiality and anonymity reasons. To draw on the direct experience of operators implementing their NIS obligations and suppliers impacted by NIS, as well as Government guidance and oversight, the spread of participants were as indicated in Table 4.

To advance academic contribution while also enhancing practical progress, this work included some action-based research to assist stakeholders in meeting their objectives under NIS and progress cooperative partnerships in cybersecurity. The semi-structured interviews and participant observation aligns well with Whyte's research methods.[38] The interviews looked at business and government priorities; the frameworks being used; and for collaboration and interaction across functional areas and between organisations. The main topics of questioning included a participant's overall experience with implementing NIS; their interaction with the supply chain and ability to control and manage it; and their processes and approach to NIS and managing suppliers.

Table 4. Summary of Research Participants.

Private Sector Participants & Roles	Public Sector Participants & Roles
OES (15 participants) Head of Digital Security Director of IT IS Security Data Protection Specialist Information Security Officer Cyber Risk & Compliance Manager OT Systems Managers	**Government Technical Advisory** (5 participants) Incident Management Product Assurance Project Manager Cyber Exercises CNI Team, Sector Leads Sociotechnical Security Group
Suppliers (7 participants) Solutions Architect Systems Integrator Cybersecurity Business Lead Product Solutions and Security Officer General Manager	**Government Policymakers** (5 participants) Cyber Resilience Policy Advisor Policy Advisor, Cyber Incentives and Regulation Cybersecurity Regulatory Policy Cyber Resilience Policy Advisor Cyber Policy Team
Sector Collaborations (4 participants) Chair of Industry Supplier Assurance Working Group Industry Association Members	**Competent Authority** (8 participants) Cybersecurity Oversight Specialist Network Security Director Cyber R&D Lead Inspector Specialist Inspector Regulation & Governance Sector Head of NIS
Consultants (3 participants) Cybersecurity Consultant Digital & Data Consultant Principal Cyber Consultant	**EU Participants** (4 participants) Information Security Expert Secure Infrastructure & Services NIS Stakeholder Reviews

4. Supply Chain Responsibility

Our interviews in particular uncovered that responsibility for cybersecurity can become blurred when there are multiple actors, components and systems involved. There is much work in progress to ensure responsibilities are defined and understood. This issue is explored here in the light of related works.

The IEC standard 62443 states that all actors have a shared responsibility for Industrial Control System (ICS) cybersecurity, including suppliers, integrators and asset owners: through secure development by suppliers; secure deploy-

ment by integrators; while asset owners configure, operate and maintain security over time.[39]

Accountability for cybersecurity remains with the operator asset owner, despite reliance on products and services from the supply chain. The operator retains responsibility for decisions made and the effectiveness of their security even if outsourcing for assessment or advice or to a cybersecurity solutions provider.[40] Where responsibility is delegated to a supplier, it is important the accountability for the effectiveness of this approach is retained within the operator. Management of the delegated responsibilities should include a requirement that cybersecurity responsibility sits at a senior level within the supplier organisation to ensure senior management support for their security responsibilities.[41]

OES identify the critical assets that their essential service depends upon. This provides a scope that the NIS Regulations can be applied to and becomes the focus for assessment and improvements.[42] However, this scope could broaden when remote maintenance is carried out or cloud-based services are used, or malicious acts affect the system whether through error or through a targeted attack. Procedures need to be in place and appropriate layers of protection implemented to ensure the defined scope is resilient when impacted from beyond the boundary of its assets.[43] Furthermore, methods for authorising connection to networks and devices or permitting changes to configurations need to be effective and appropriate in a real time operational environment.

5. Cooperation in Managing Supply Chains

While cybersecurity capability can be built into products, the end-to-end integrated solution needs to be effectively secured involving people, processes and technology. There is an inherent need to integrate skillsets to achieve cybersecurity. Implementing the NIS Directive has necessarily involved bringing together different parts of an organisation to identify the assets in scope and set in place a continuous process for protection, detection, response and recovery. Ideally, this requires a synthesis of IT and OT expertise with sector specific knowledge and in addition the suppliers' deep knowledge of their products and services. The following section explores insights from supply chain management literature on coordinating and influencing supply chains.

5.1 Building Collaborations

Appropriate collaborative strategies involve both social and technological concerns to meet technical requirements and integrate relevant processes between the organisations involved. Building inter-organizational relationships with suppliers is something to be fostered over time to motivate their participation in collaborative behaviours. Such collaborative effort provides a considerable mediating role in achieving supply chain performance.[44] Several industry interviews shared the opinion that if they had to resort wholly to contractual agreement, it would feel like a failure. Their emphasis, particularly with critical suppliers, was on a mutually supportive relationship and a trusted partnership.

This mirrors a study of international procurement where contracts were in place in most cases but were considered less important than clear communication to agree common perceptions and expectations throughout the relationship. Close working relationships were more important than a contract in effective partnership over time. A mutual commitment showed the potential to achieve more than formal agreements.[45]

Instead of suppliers acting with self-interest in supply chain systems, Shin and Park demonstrate the importance of a broader awareness of a supply chain system and a mature partnership development to achieve greater confidence in the resiliency of the supply chain. They identify the following attributes as desirable for all supply chain members and forming key elements of resilience capability and improving a firm's ability to recover from unexpected events:

- common interest, a collective goal, going beyond self-interest
- mutual respect among supply chain partners, competencies and potential for achievement are recognised
- deepening trust, meeting operational standards, displaying goodwill towards the partnership
- Interaction obligations, participation in formal and informal communications among partners for supply chain management activities. A lead firm influencing actions and behaviours of supply chain members to improve capabilities.[46]

Rather than raising maturity level generally, it is important to align improvement in capability with the actual risk exposure to ensure investments are proportionate, i.e., through matching the level of risk and vulnerability with appropriate capability to focus investment and effort on actual resilience gaps.[47] This concept of a balanced resilience has also been extended to include the supply chain network.[48] However, there are challenges in knowing the actual risk exposure and the likelihood of incidents and proving whether a cybersecurity investment has been a worthwhile prevention, particularly if there is an absence of incidents. Cooperation is important to bring together information on the latest trend of attacks, along with an understanding of the potential impact, and having preventions in place to minimise these types of impact.

5.2 Reducing Overhead of Supply Chain Coordination

Attempting to control entire supply chains of cyber secure activity would be a vast and costly undertaking. A more achievable endeavour is to strategically decide what aspects to control and what to let emerge. Choi points out the differences between control and emergence in managing supply chains as complex adaptive systems. The use of control mechanisms involves a formal oversight of suppliers with contractual arrangements and adherence to common standards for more predictable outcomes. Emergence, on the other hand, is where more autonomy is given for local decision making and emergence of the required outcomes is encouraged through positive feedback. Choi proposes, that companies managing their supply networks through both control and emergence, outper-

form those that focus on only one of these approaches. This entails controlling the overall direction while remaining vigilant in observing what emerges, to make appropriate decisions and changes. Also, encouraging creativity and adaptability in the supply network reduces the coordination cost of a supply network. Choi suggests controlling several tiers deep only for a few critical areas and otherwise allowing the supply network to emerge through empowering top tier suppliers to manage their suppliers.[49]

Pass through clauses in contracts with Tier 1 suppliers require the supplier's suppliers to have the same protections in place and the contracted supplier is held responsible for compliance with this clause. These clauses typically only reach Tier1 and Tier 2 suppliers.[50] Coordination of a 'cluster' of suppliers is more realistic than oversight of multiple tiers in the supply chain. Via a lead organisation this is coordinated from a strategic level with a focus on capability and agreed goals, using metrics as an enabler.[51] Roseira's research into supplier networks identifies the ability to recognise the potential in each supplier relationship and diffusing this to other supplier relationships as being of central importance in managing portfolios of suppliers.[52] Addressing actors beyond Tier 1 of the supply chain through interactions among multiple actors in a supply network more commonly leads to resilience to supply chain events.[53]

The interconnectedness of supply chain actors requires a holistic approach to resilience. Knowledge created and shared among supply chain partners to build a 'capacity to adapt' to continuous change will allow the whole supply chain to become more resilient. Colicchia recommends "a holistic and extended approach." Awareness training should go beyond the boundaries of the workplace to appreciate the extent of impact because human behaviours can affect the whole supply chain network.[54] Keegan recommends creating opportunities for cooperation among private sector organisations and public-private cooperation through government involvement in industry working groups, creating forums to enable collaboration across organisations and countries.[55] Examples of such collaboration are described in Section 6.

6. Perspectives on Implementing NIS

6.1 Policy Perspective

Government departments have defined responsibilities and set expectations by providing NIS Guidance and a Cyber Assessment Framework (CAF). By describing indicators of good practice,[56] the CAF shows the outcomes to be achieved within each of the principles previously shown in Figure 1.

The evidence supporting the original NIS intervention showed that only 13 % of organisations were setting cybersecurity standards for their suppliers to meet; and during 2017 19 % had experienced a breach that resulted in a material loss.[57] The potential benefits expected from implementing the NIS Directive, at the outset in April 2018 included the following[58]:

- a reduction in risks to essential services due to the improved security level

- to improve the cybersecurity of network and information systems (NIS) underpinning essential services
- to reduce the likelihood and impact of security incidents
- to also reduce breaches/attacks that are below the Directive thresholds
- a 5 % reduction in number of organisations with a breach or attack was assumed
- common security requirements for all market operators
- the exchange of information and coordination of actions
- to improve advice and incident response for OES through international cooperation and information sharing
- extended benefits were expected to be "substantial where even just one significant incident is prevented" due to potential impact on the wider economy if essential services and network and information systems become unavailable.

There was an emphasis on number of incidents and an expectation that implementing the NIS principles would reduce the number of incidents. However, it was also observed that it is difficult to determine whether implementing security measures will result in a reduced number of breaches. The cybersecurity breaches survey of 2020 shows that breaches and attacks have increased in the last three years.[59] Industry feedback during the NIS Review also confirmed the cyber threat level has increased. Fewer negative impacts have been experienced from those breaches so the resilience to attacks appears to have improved, however continuous improvement is not evidenced, with policies and processes put in place to meet new regulations being maintained rather than enhanced.[60]

In 2020, the UK proposed some amendments to their NIS Regulations that showed a move away from penalties. The penalty bands have been revised and a notice of intention to impose a penalty must be given by CA first. This preference was also expressed in interviews through discussion of the "use of regulatory judgement" while assessing compliance and the intention to "lead with a carrot more than with a stick." The supply chain issues have a wider impact than just NIS organisations, so policymakers are looking separately at the role of government in reducing supply chain risks at scale, and what would constitute effective support from government with managing the supply chain risks that OES are currently responsible for.[61]

6.2 Regulator Perspective

This section describes the general perspective of CAs, gathered from our interviews, along with some examples of specific approaches. Utilising the CAF from NCSC and based on likely threat scenarios, CAs set expectations on OES with a CAF profile for their sector, using red/amber/green notation to highlight the priorities to be achieved. CAs assess the performance of OES to decide a priority for audits and inspections. A range of parameters are used for this, including:

- likely consequences or impact of an OES being non-compliant
- safety considerations
- self-assessment of OES
- previous knowledge of the facility
- size of facility and importance to the sector.

One CA is using a matrix approach to assess the complexity of different facilities. They assign a complexity level to decide which sites they need to audit. They also decide how much time each facility 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.

CAs expect operators to be actively sourcing threat information, to having ongoing vulnerability and threat awareness and a decision-making process to consider new threats at the level of impact. The consequences of new threats are considered alongside measures that are in place to decide necessary improvements and likely effects. The end user is expected to tie it all up, the supply chain vulnerabilities and latest threat intelligence into a potential impact on their deployment environment, to conclude how to respond.

CAs consider a range of parameters when assessing sites including the safety impact for the site and the community around. They inspect their NIS sites against all the NIS contributing outcomes from A1a through to D2, relative to the CAF profile they have set for their sector. An example from one CA shows each site is given a score and the extent of their NIS compliance is assigned a category from 1 to 6 as shown in Table 5. The scores help to decide appropriate enforcement levels, for example where compliance has some gaps, a letter specifying actions to be resolved is provided with follow up to ensure actions are implemented. Where compliance is poor, formal legal powers are exercised to enforce the required compliance. 'Regulatory judgment' is also applied to their response, through the CA knowing the site history, realistic expenditure such that an agreed approach can be reached.

The supply chain aspect is in its early stages of maturity. NIS sites broadly know who their suppliers are, and are setting baseline requirements with control system and safety system vendors but these are not in contracts; yet formal assurance of suppliers is work in progress. Big suppliers of control and safety systems have a strong awareness of how cyberthreats can affect their equipment. More recent control systems installations have security included by default. There is less understanding among sites on how to improve security around legacy systems. Actions and enforcements have enabled changes in this area to improve processes and network architecture, with OES engaging with their supply chain as they progress.

There is a wide range of situations with the sites, some more proactive or with more resources to improve compliance, others tend to wait for CA visit and then make the necessary changes. Some sites are heavily committed to one supplier, using the same vendor for control and safety systems for an integrated

Table 5. Example of NIS Compliance categories being used by CA.

OES Score	OES Category	Consequence from CA
10	Beyond NIS Compliance	
20	Fully NIS Compliant	
30	Broadly NIS Compliant	Action to resolve
40	Poor Compliance	Action to resolve
50	Very Poor	Formal enforcement
60	Unacceptable	Formal enforcement

solution and consistency with support and spares. Other sites are using a range of equipment requiring systems to be integrated by a different supplier and involving a more disparate and complex cybersecurity solution.

Despite a quantity of outsourcing, the legal duty for cybersecurity sits with the OES. They are expected to be an 'intelligent customer,' to know enough to ask the right questions and set the required expectations on suppliers. This can be challenging for smaller sites with fewer resources for this.

In some cases, it comes down to one person having responsibility for safety and security, managing changes and making improvements and also being competent in 3rd party assurance.

While most vendors and suppliers have some understanding of cybersecurity issues and that they need to be aware of vulnerabilities in their systems, the regulation has been necessary to push the end users into setting this into contractual arrangements. Some level of standardisation of expectations on the supply chain would be useful, as the range of issues is largely similar for end users and suppliers. A certification process would assist end users to understand the security capability in products and services they are using and demonstrate assurance of vendor solutions through validation by an independent entity. The EU Cybersecurity Act is introducing a scheme to certify devices and services. This will involve third party certification of ICT products at two security assurance levels: 'substantial' and 'high.' It also includes certification of Protection Profiles, being an implementation-independent set of security requirements.

6.3 Perspectives of Operators of Essential Services (OES)

Operators of Essential Services (OES) are implementing the NIS principles and are required to report incidents that affect the delivery of their essential services. Our interviewees expressed that having obligations under the NIS Directive has given OES a strong focus to improve their cybersecurity capability and raise awareness in their organisations and essentially to achieve support at Board Level for making the necessary improvements. Nevertheless OES, in general, have limited resources for overseeing supply chain risks and, as individual organisations, can often lack negotiating power with suppliers.[62]

OES are managing cybersecurity across multiple suppliers and updating supplier contracts is a gradual process. Their visibility of supply chain cybersecurity is limited such that incidents in the supply chain may not be notified to an OES.

In some cases, there is a low cybersecurity maturity among available suppliers or even dependency on a single supplier for essential product. OES working individually appear to lack real influence to demand greater levels of assurance. In addition, improving the diversity of suppliers may not be more resilient if different suppliers share common components or the same operating system.

During the procurement process, questionnaires are sent to potential suppliers to understand their cybersecurity maturity level. The suppliers' responses are considered, alongside other business risks, during procurement decisions. The questionnaires being used are predominantly assessing a supplier's cybersecurity posture as a company by looking at how cybersecurity risks are managed; if security policies and processes are implemented; and how effective they see their cybersecurity controls to be.

However, the residual risk that the OES is carrying relates to their cyber risk in operation so the cyber-assurance of the supplier's product or service needs to be the focus, more than the supplier company itself. These questionnaires are informing risk decisions inside the operator on criticality and importance. It is therefore necessary to look at the context of an OES deployment and the impact a supply chain event would have in this specific OES environment, and to know how important that product or service is to the business function and to establish the extent of dependency on that supplier. By also looking at the degree of access a supplier has to sensitive assets, this further paints the picture of how exposed an OES is to a supplier's cyber risks.

Table 6 highlights the key challenges discovered in our interviews that OES face in securing their supply chains to comply with NIS. Due to the limited influence, an OES has working at this on their own, there has been a growing interest

Table 6. Supply Chain challenges of OES.

Key challenges faced by OES in securing Supply Chains
OES have a limited ability to negotiate security requirements from suppliers.
OES lack choice in selecting suppliers – they shoulder the risk of low cybersecurity maturity among available suppliers.
Difficulty obtaining supplier commitment to improvements following risk assessments.
Facing challenges with inserting cybersecurity requirements into established contracts at renewal.
Limited resources to integrate cyber security requirements and expectations into all outsourced activities.
Visibility of sub-contractors is very limited.
Supply chain incidents may not be notified to the OES.
Uncertainties around security status of products – there is lack of transparency on through life support.
Uncertainties over shared responsibilities in operations, complex dependencies.

to collaborate. For example, to discuss shared security requirements that could be built into suppliers' offerings rather than cybersecurity add-ons being sold separately to each OES; to have cybersecurity included in technical requirements so that the fundamentals are in place and it is priced with cybersecurity included. OES are looking for support beyond initial warranty, for the life of an asset. There is a lack of clarity and transparency on the through life support for the security of products leaving uncertainties around the security status of products. While the Operators of Essential Services are the necessary focal point of NIS, it is a complex task for OES to assign appropriate requirements and responsibilities onto suppliers and systems integrators. Suppliers are also receiving multiple different questionnaires from different operators to assess their cybersecurity capability which is reducing the efficiency of supply chain assurance activity for all parties.

While NIS has brought a one company approach to improving cybersecurity one OES at a time, there are areas where a combined approach needs to be facilitated. It would involve a significant overhead of cost and time for each OES to attend to the cybersecurity of their entire supply chain, or even just the critical suppliers on which their essential service depends. The NIS implementation has mobilised some collaborations to work towards NIS outcomes more effectively, highlighting the importance of partnership to achieve cybersecurity. Recent working groups have been fostering collaborations to this effect. These are described in Section 7.

6.4 Supplier Perspective

The weighting of this perspective is towards suppliers with a strong presence in CNI and who are focussed on cybersecurity; hence, they were more willing to participate in interviews. Table 7 outlines some of the key challenges raised by suppliers.

Suppliers that offer a good standard of cybersecurity in their offering can be penalised when cybersecurity is considered, but not prioritised, in the procurement process and where there is an emphasis on keeping costs down. Also,

Table 7. Challenges experienced by Suppliers.

Key challenges faced by Suppliers
Suppliers are receiving multiple different questionnaires from different operators to assess their cybersecurity capability.
Cybersecurity is considered by OES but not prioritised in their procurement process.
An emphasis on keeping costs down is encouraging an installation that is right for today rather than future proof infrastructure.
Where cybersecurity requirements are not adequately defined by OES, suppliers are left to estimate the risk appetite and cybersecurity level they need to meet for their customer's context.

where cybersecurity requirements are not adequately defined by OES, suppliers are left to estimate the risk appetite and cybersecurity level they need to meet for their customer's context.

Suppliers need OES to agree and provide common requirements per sector to ensure basic security is in place across all supplier offerings. OES jointly agreeing and providing common security requirements in one sector has been very well received by suppliers. For that sector, it created a more level playing field and a standard expectation that prevented a race to the bottom on security for best cost solution. Suppliers are showing a preference for their market being driven by the cybersecurity requirements per sector, defined by OES. However, even at the requirements stage, OES can require dialogue with their suppliers in order to fully define their requirements, to bring a supplier's deep knowledge of their product together with operator's understanding of the environment it is deployed into. There are concerns among OES that their security requirements could force a significant technology change. Large suppliers know their equipment is embedded into an OES so they can charge for security improvements because it would be a massive undertaking for the OES to change supplier.

Suppliers are seeing an increasing interest in having cybersecurity capability within their products coming from the manufacturing sector. However, in NIS regulated sectors, they see a cultural aspect that is slowing down cybersecurity improvements. In particular, there is an intense focus on costs in one sector that encourages an installation that is right for today, rather than deploying future proof infrastructure. Where cybersecurity responsibility has been given to IT, there can be a limited understanding of the extent of their cybersecurity responsibilities within the operational environment.

While the responsibility for implementing and complying with the NIS Directive is with the OES, there is reluctance from suppliers to take on cybersecurity responsibilities that sit in the context of OES deployments. However, there needs to be a fair set of expectations on suppliers for example to have cybersecurity designed into their products and services and the OES take responsibility for how cybersecurity capability is configured and used in their environment. Some collaboration and negotiation will be required to agree what can be expected and included as standard within a supplier offering and what is considered as additional and chargeable as an extra. Both the operators and suppliers need more clarity on the cybersecurity practices to adopt and a shared understanding of the current and emerging cybersecurity risks, as increasing digitalisation progresses.

7. Examples of Interorganizational Cooperation for Cybersecurity

Two-way relationships between operators of critical infrastructure and the suppliers of products and services they use are an important consideration. Cyber security issues in the supply chain can introduce risks and potential operational impact that the operator needs to manage. An operational incident could also impact the reputation of a supplier. The translation of an operator's regulatory

obligation into security requirements of suppliers can to some extent be incorporated into commercial contracts and in this way allocate some responsibilities to suppliers. A continuing relationship with suppliers is necessary to support cybersecurity needs such as patching of software and incident response arrangements and particularly throughout the lifecycle of products. Consideration of how the relationship will endure over time, the potential needs in the longer term and how they can be met through likely changes.[63]

7.1 Unified Supply Chain Assurance

Although the focus of this paper has been on the UK response to NIS implementation, the concerns extend across national borders. For example, the European Air Traffic Management (ATM) industry has worked together to produce a unified approach to supply chain assurance. Table 8 shows the supply chain aspect of the maturity model that was developed to compare the suppliers to Air Navigation Service Providers (ANSP). The levels define a progression from partial to full oversight of suppliers, and from self-assessment to carrying out compliance checks. The eventual aim is to achieve an adaptive security that supports regular updates to requirements and independent assessments of suppliers.

Figure 3 provides an example for presenting the comparison of suppliers in order of maturity. The intention was for ATM operators to progress towards achieving full oversight of their supply chain by following this unified approach. Since the introduction of this unified maturity model and the NIS obligations, there has been some progress with the oversight of supply chains through achieving a partial understanding of supplier maturity. However, to take actions

Table 8. Supply Chain category of ATM Maturity Model.[64]

Supply Chain Risk Management	
The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has in place the processes to identify, assess and manage supply chain risks. Appropriate levels of trust are established with data exchange partners.	
Level 0 non-existent	No complete overview of all suppliers / partners.
Level 1 partial	Some requirements placed on some suppliers and agreements with some partners; partial and informal understanding of supplier/partner cyber- maturity.
Level 2 defined	Minimum set of requirements placed on all critical suppliers and agreements with partners, with mostly self-assessment for compliance.
Level 3 assured	Requirements placed on suppliers with proportionate compliance checks and processes / penalties /measures for non-compliance.
Level 4 adaptive	Independent reviews / audits / assessments supporting regular updates of requirements against new good practices.

Function	Category	ANSP	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5
LEAD AND GOVERN	Leadership and governance	3	3	3	2	1	1
	Cyber Security Management System (CyberSecMS)	2	3	2	2	2	1
IDENTIFY	Asset Management	4	4	3	2	2	1
	Risk Assessment	1	3	3	1	2	1
	Information sharing	2	3	2	1	1	0
	Supply Chain Risk Management	2	3	3	2	1	0
PROTECT	Identity Management and Access Control	3	4	2	2	3	2
	Human-centred security	1	3	3	2	2	0
	Protective Technology	3	4	2	3	1	1
DETECT	Anomalies and Events	3	2	2	2	2	0
RESPOND	Response Planning	2	3	3	3	0	0
	Mitigation	3	3	2	2	0	1
RECOVER	Recovery Planning	3	3	3	1	2	1

Figure 3: Unified approach to supply chain assurance for ANSP.[65]

towards improvement required a gathering of the key issues from operators so that visits and workshops with key suppliers could be arranged at a country level coordinated by the CAA.

7.2 Collaborative Supplier Assurance

The effective implementation of the NIS Directive and resulting improvement in cybersecurity across critical infrastructure is contextually dependent on the knowledge of each operator's own environment and unique deployment of infrastructure. The necessity of focusing the NIS Directive on the activities of individual organisations has produced an array of individual responses. This was an important aspect of the NIS Guidance, by providing outcomes to aim for rather than a checklist of actions to ensure the efforts were towards the reduction of risks for each operational facility. As this effort rippled out, a knock-on effect to suppliers was receiving multiple different questionnaires from their customers to assess their cybersecurity.

This overhead of activity, for both OES and suppliers, to understand the risks in the supply chain can be reduced through improved cooperation. Groups of OES in the energy sector were discussing their common security requirements with suppliers, one at a time. This developed into a supplier assurance working group to agree a common approach for the whole energy sector, supported by Government. This collaboration has produced and agreed a set of guidance for the sector on supplier assurance. This working group is also working on a code of practice and partnership approach with suppliers to the energy sector.

Sector collaborations can improve OES leverage with larger suppliers. Agreement of common security requirements per sector by OES can provide a more level playing field for the supplier market. Defining clear security requirements at a whole sector level should improve negotiations with sole suppliers to meet them, despite not having the competition within the market to improve their security provision. Where possible, a more centralised coordination of supplier assurance is recommended by introducing a shared assessment process within each sector with one assessment per supplier to improve efficiencies in this

area. A trusted intermediary in such partnerships has been particularly effective to establish a picture for the sector, by anonymising information from individual OES.

7.3 Centralised Supplier Assurance

The Scottish Government have provided an example of a centralised supplier assessment process within the health sector through their digital telecare security assessments.[66] The key aims and outcomes have been as follows:

- for consistency and to reduce the burden of providing evidence to multiple parties
- to increase supplier engagement
- to reduce the cost of supplier assurance
- to use a risk-based assessment of product/service and supplier company
- to build trust between the assessor and suppliers
- to establish a non-disclosure agreement due to vulnerabilities identified during the assurance process
- to offer guidance, as necessary, for suppliers to achieve the required standard
- to agree timely improvements where required.

7.4 Managing Software Vulnerabilities

Complex supply chains can propagate vulnerabilities. Without a software bill of materials (SBOM), it is more difficult to know if vulnerable software is in a device. Risk mitigation requires a detailed and dynamic asset inventory to hold information for each device, on vendors, operating system, firmware version etc. The risk surface also depends on the context surrounding a device so the actual impact of a vulnerability depends on the environment a targeted device is implemented in.[67]

New software vulnerabilities can be embedded within many components and users need to know if they will be affected by a software vulnerability through regular assurance of a SBOM. SAFEcode produced an assurance model that includes:

- security – anticipate and address vulnerabilities during design
- integrity – in sourcing and creating software components, address the likelihood of vulnerabilities in delivery of software
- authenticity – provide ways to assure and differentiate genuine products from counterfeit products.[68]

Edison Electric Institute (EEI) with U.S. Department of Commerce's National Technology and Information Administration (NTIA) is at the nexus of a discussion with software vendors, security experts and asset owners. NTIA are facilitating this effort with different sectors: health, energy, automotive and banking with an emphasis on cooperation rather than using regulations. This involves

the application of SBOM as a tool to minimise supply chain risks, to know the components of software so that vulnerabilities become known and to work with suppliers to mitigate them. Sector specific engagement will uncover the importance of an element to that sector and potential impact to a sector of a vulnerable supply chain component. Cross sector engagement will also be necessary because different CNI sectors are likely to have the same software components embedded in their systems. The intention is to develop a shared vision and language working with individual sectors first and to work towards creating machine readable methods for fast automatic assessment of impact and to enable sharing across sectors.[69]

7.5 Cyber Exercises with Suppliers

A recent victim of attacks reported that exposure to incidents has significantly increased awareness across the organisation. Any phishing attempt "echoes" through our organisation, sharing of near misses or potential incidents happens much faster. Exercises in responding to cybersecurity events can provide a holistic experience to identify capability gaps from people, process and technology perspectives. Whole sector cyber exercises have increased awareness of the need to respond collectively to cyber events and the benefits of collaborative working across OES, suppliers and government. Participants in the cyber exercises appreciated gaining visibility of the bigger picture and understanding of how local decisions can impact the wider sector. It exposed the need for a coordination role, by Government or an industry body, to deal with sector wide incidents, rather than being treated as several incidents by many separate organisations. It raised supplier awareness of the necessity to support CNI with NIS compliance and even to revisit contractual agreements with individual OES to consider extending them in some areas towards whole sector agreements.

8. Enhancing Cooperation in Securing Supply Chains

In addition to specific NIS Guidance, the UK NCSC provide general supply chain security guidance to improve overall resilience and reduce business disruptions.[70] This is offered in four stages as listed in Table 9. Our research recommends some enhancements to this guidance, based on the experiences of implementing NIS across critical infrastructure, that are listed in Table 9 and elaborated below. These recommendations aim to improve effective interworking across supply chains.

Table 9. Enhancements to Supply Chain Guidance.

NCSC Supply Chain principles	Enhancements to Supply Chain Guidance
Understand the Risks	Emphasis on risk reduction
Establish Control	Driving improvements
Check your arrangements	Measures & Performance
Continuous improvement	Mutual Commitment & Accountability

8.1 Emphasis on Risk Reduction

Rather than an emphasis on increasing maturity or adding capability, it is important that decisions continue to be based on reducing risks and minimising the impact of incidents. To really know and understand the supply chain risks to critical infrastructure requires improved information sharing and cooperation across industry and across supply networks. This would assist with understanding the latest threat picture, of incidents and near misses, and with identifying the impact of vulnerabilities at a sector level, such as software vulnerabilities in supply chain components.

In addition to the emphasis on managing and reducing risks for the assets relevant to delivering essential services, further attention could be given to the impact beyond NIS identified assets, by considering the cyber resilience of the entire organisation, as a whole, to include the human and process effects on these critical assets and the delivery of essential services.

8.2 Driving Improvements

While the NCSC supply chain guidance places attention on establishing control of the supply chain, this research has highlighted some challenges for OES working alone with achieving that level of control. Therefore, balancing controls with cooperation is recommended and approaches to achieving this have been explored. It is essential to establish the new behaviours that will drive improvements and reduce the risks. Sector collaborations can improve OES leverage with suppliers. For example, by OES together agreeing common security requirements, to lead their sector's supplier market. A combined supplier assurance process can also reduce the overhead of this activity on both OES and suppliers. More resources will be required to consider essential components of the supply chain and to facilitate an assured software bill of materials SBOM and know the impact of vulnerabilities in supply chain elements.

In addition to holding an asset inventory that covers hardware, software, and connectivity to support security initiatives such as patching and assessing impact of vulnerabilities, an inventory of supplier relationships is recommended to cover the human and process elements as well and recognise the supply chain as a strategic asset to be managed. Again, sector wide cooperation could establish the foundation for ongoing relations with suppliers through agreeing a sector code of practice. The individual operator-supplier relationships can then focus on more contextual needs related to OES deployments in their unique operational environments.

Understanding the areas of commonality indicates what can be achieved collectively per sector. This will require Government support for the necessary collaborations, for example cyber exercises involving suppliers to improve integration of incident response processes. Governments can positively impact the long-term goal of cybersecurity improvements by supporting or facilitating such interorganizational cooperation.

8.3 Measures & Performance

A collective responsibility and mutual commitment to cybersecurity is the means to establish the required behaviours and improvements. By understanding the potential impact of supply chain components on CNI, suppliers can be categorized as critical, important, medium or low priority.[71] In order to track and measure improvements, points of governance or points of influence need to be identified within the supply network, where controls or cooperation are required with critical and important suppliers.

Similar to the six-monthly review of NIS improvement plans with OES that are overseen by the CA, there also needs to be a regular review of commitments to maintain accountability with suppliers. To be more efficient on time and resources, and with the required interorganizational cooperation in place, this can largely be an attention to sector wide commitments from the supply chain. Then individual OES attention can be on their more contextual and tailored requirements. Agreeing shared language will also be necessary to facilitate the collaboration across organisations.

Table 10 shows examples of actions that all depend on effective cooperation. Using a balance of lagging and leading measures to assess performance and guide improvements, will inform future decisions while learning from events.

Table 10. Cooperation in performance.

Lagging indicators to learn from the past:	Leading indicators to inform decisions:
• Reporting of incidents and their impact • Ability to recover from events • Sharing of lessons learned to plan improvements • Responsible disclosure of newly discovered vulnerabilities • Tracking the resolution of vulnerabilities or the required mitigations	• Knowing what to improve, improvement plans assessing performance. The subjective assessments assigning red, amber or green could instead be linked to more specific and measurable milestones in the improvement plans • Consider what-if scenarios and potential disruptions, emerging threats, early signs of vulnerabilities, and near misses. This needs improved coordination and cooperation to guide these preparations • Improved visibility of dependencies on supply chain components, to prevent supply chain effects cascading • Understand the residual risks being carried by OES to prioritise their mitigation

8.4 Mutual Commitment & Accountability

Figure 4 demonstrates the collective commitment that is required across public-private partnerships involving OESs, Suppliers and Government departments.

A code of practice per sector would establish the commitment to action. A definition of and regular review of commitments will maintain accountability among sector participants. For example, broadening the current individual OES improvement plans by also overseeing sector improvements and mutual commitments in the interorganizational space. In the longer term, it is a continual adaptation to the evolving situation, by the whole supply chain network, that will improve resilience to cyber events.

9. Conclusion

This paper has evaluated public and private sector experiences with implementing the NIS Directive, and provided examples of effective cybersecurity collaborations. It has presented some enhancements to supply chain guidance to assist with reducing cybersecurity risks to critical infrastructure and emphasizes the need for greater interorganizational cooperation.

In particular, the OES context of deployment and operational impact makes it harder for OES to share cybersecurity responsibility with suppliers for products and services that OES are hosting in their own operational environment. The ability of OES to make formal upfront arrangements with suppliers through contractual agreements is limited, not least due to the adaptability to an evolve-

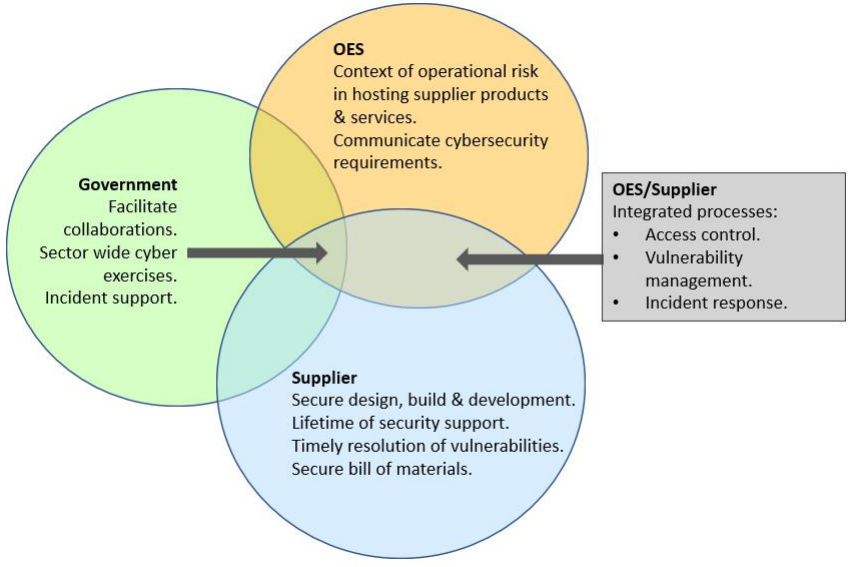

Figure 4: Mutual Commitment required from Public & Private actors.

ing situation that is required. Fostering trusted partnerships and mutual commitments is equally important and even has the potential to achieve more than formal agreements.

The regulatory controls introduced by NIS need to be balanced with a more cooperative approach through Government support for the necessary collaborations that will drive improvements. It is also important that common language, standards and frameworks are used to promote shared understanding along the supply chain. To incentivise suppliers, a greater clarity on sector cybersecurity requirements is needed to set the level and lead supplier markets.

This research recommends a combination of control and cooperation mechanisms, developed from researching industry experiences and supported by supply chain management literature. Future work will evaluate the effectiveness of industry working groups cooperating across public and private organisations to improve cybersecurity. We are also concerned to validate our arguments by more detailed interviews and focus groups with stakeholders across Europe and beyond as nations across the world struggle to address shared problems of supply chain assurance in national critical infrastructures. Future research will include a capabilities-based engineering analysis to investigate the effective engagement of sector wide supply networks in continuous adaptation to cybersecurity.

To build and maintain the required cybersecurity capability to secure essential services and refine those capabilities in the light of new threats and vulnerabilities, organisations, products, and services must understand their role in critical infrastructure and their place and responsibility in the supply chain.

Acknowledgement

This work was supported and funded by the Research Institute of Trustworthy Inter-connected Cyber-physical Systems (RITICS) and the UK NCSC.

References

[1] European Commission, “Directive (EU) 2016/1148 of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union,” *Official Journal of the European Union*, 19 July 2016, accessed March 24, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

[2] European Commission, “Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Rrepealing Directive (EU) 2016/1148,” Brussels, 2020, accessed March 24, 2021, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive.

[3] National Cyber Security Centre, *NIS Guidance Collection*, 2018, accessed March 24, 2021, https://www.ncsc.gov.uk/collection/caf.

[4] National Cyber Security Centre, *NIS Guidance Collection*, 2018, accessed March 24, 2021, https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance.

[5] NCSC, *Cyber Assessment Framework V3.0*.

[6] NCSC, *Cyber Assessment Framework V3.0*, 2019, accessed March 24, 2021.

[7] NCSC, *NIS Guidance Collection*, 2018.

[8] NCSC, *Cyber Assessment Framework V3.0*.

[9] Tom Kellermann, "The Ominous Rise of "Island Hopping" and Counter Incident Response Continues," White Paper, VMware Carbon Black, September 2019, accessed May 4, 2021, https://www.carbonblack.com/resources/the-ominous-rise-of-island-hopping-counter-incident-response-continues/.

[10] National Cyber Security Centre, *CAF Supply Chain Guidance.* 2019. Accessed February 18, 2021, https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a-4-supply-chain.

[11] Luca Urciuoli, Toni Männistö, Juha Hintsa, and Tamanna Khan, "Supply Chain Cyber Security – Potential Threats," *Information & Security: An International Journal* 29, no. 1 (2013): 51-68, http://dx.doi.org/10.11610/isij.2904.

[12] Shipra Pandey, Rajesh Kumar Singh, Angappa Gunasekaran, and Anjali Kaushik, "Cyber Security Risks in Globalized Supply Chains: Conceptual Framework," *Journal of Global Operations and Strategic Sourcing* 13, no. 1 (2020): 103-128, https://doi.org/10.1108/JGOSS-05-2019-0042.

[13] BlueVoyant, *Managing Cyber Risk Across the Extended Vendor Ecosystem*, 2020, accessed May 4, 2021, www.dvvs.co.uk/wp-content/uploads/2020/12/BlueVoyant-Supply-Chain-Cyber-Risk-Global-Report-LRES.pdf.

[14] Anthony Spadafora, *Energy Giant EDP Hit with RagnarLocker Ransomware,* techradar.pro, UK edition, 2020, accessed March 28, 2021, https://www.techradar.com/uk/news/energy-giant-edp-hit-with-ragnarlocker-ransomware.

[15] Malwarebytes Threat Intelligence Team, "Honda and Enel Impacted by Cyber Attack Suspected to be Ransomware," June 9, 2020, accessed March 28, 2021. https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/; Alina Georgiana Petcu, "Netwalker Ransomware Explained: What You Need to Know," September 9, 2020, accessed March 29 2021, https://heimdalsecurity.com/blog/netwalker-ransomware-explained/.

[16] Amin Hassanzadeh, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and M. Katherine Banks, "A Review of Cybersecurity Incidents in the Water Sector," *Journal of Environmental Engineering* 146, no. 5 (2020): 03120003.

[17] Steve Kardon, "Florida Water Treatment Plant Hit with Cyber Attack," Industrial Defender, February 9, 2021. accessed March 29, 2021, https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/.

[18] Bert Willemsen and Menno Cadee, "Extending the Airport Boundary: Connecting Physical Security and Cybersecurity," *Journal of Airport Management* 12, no. 3 (2018): 236-247.

[19] Chris W. Johnson, "Preparing for Cyber-attacks on Air Traffic Management Infrastructures: Cyber-safety Scenario Generation," 7th IET International Conference on System Safety, incorporating the Cyber Security Conference, Edinburgh, UK, 15-18 October 2012, https://doi.org/10.1049/cp.2012.1502.

[20] Lily Hay Newman, "Russia's FireEye Hack Is a Statement—but Not a Catastrophe," *Wired*, August 12, 2020, accessed March 27, 2021, www.wired.com/story/russia-fireeye-hack-statement-not-catastrophe/; Eduard Kovacs, "SolarWinds Says 18,000 Customers May Have Used Compromised Orion Product," *SecurityWeek*, December 14, 2020, accessed March 26, 2021, www.securityweek.com/solarwinds-says-18000-customers-may-have-used-compromised-product; Gordon Coreraand Joe Tidy, "US Treasury and Commerce Department Targeted in Cyber-attack," *BBC News*, December 14, 2020, accessed March 26, 2021, https://www.bbc.co.uk/news/world-us-canada-55265442.

[21] Jason Sattler, "Significant Attacks on Microsoft Exchange ProxyLogon Detected," *F-Secure*, March 19, 2021, accessed March 25, 2021, https://blog.f-secure.com/microsoft-exchange-proxylogon/.

[22] Josh Fruhlinger, "Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?" CSO, February 12, 2020, accessed March 26, 2021, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

[23] Sonatype, "2020 DevSecOps Community Survey," accessed March 26, 2021, https://www.sonatype.com/2020survey.

[24] Sonatype, "2020 State of the Software Supply Chain Report," August 12, 2020, accessed May 3, 2021, https://www.sonatype.com/campaign/wp-2020-state-of-the-software-supply-chain-report.

[25] UK Cabinet Office & Detica, "The Cost of Cyber Crime," 2011, accessed 3 May 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

[26] Ponemon Institute & Accenture Security, "The Cost of Cybercrime," 2019. www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

[27] Department for Digital, Culture, Media & Sport, "Cyber Security Breaches Survey 2020," accessed May 3, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf.

[28] Theresa Sobb, Benjamin Turnbull, and Nour Moustafa, "Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions, *Electronics* 9, no. 11 (2020): 1864, https://doi.org/10.3390/electronics9111864.

[29] Shannon Eggers, "A Novel Approach for Analyzing the Nuclear Supply Chain Cyber-Attack Surface," *Nuclear Engineering and Technology* 53, no. 3 (2021): 879-887, https://doi.org/10.1016/j.net.2020.08.021.

[30] Abel Yeboah-Ofori and Shareeful Islam, "Cyber Security Threat Modeling for Supply Chain Organizational Environments." *Future Internet* 11, no. 3 (2019), 63, https://doi.org/10.3390/fi11030063.

[31] Nikolaos Polatidis, Michalis Pavlidis, and Haralambos Mouratidis, "Cyber-attack Path Discovery in a Dynamic Supply Chain Maritime Risk Management System," *Computer Standards & Interfaces* 56 (2018): 74-82, https://doi.org/10.1016/j.csi.2017.09.006.

[32] IEC62443-2-4. "Security Program Requirements for IACS Service Providers," accessed May 4, 2021. Preview is available at https://webstore.iec.ch/preview/info_iec62443-2-4%7Bed1.1%7Den.pdf.

[33] ENISA, *Guidelines for Securing the Internet of Things*, November 9, 2020, accessed May 4, 2021, https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things.

[34] Oleksandr Polischuk, "Ecosystem Platform for the Defence and Security Sector of Ukraine," *Information & Security: An International Journal* 45 (2020): 7-19, https://doi.org/10.11610/isij.4501.

[35] Georgi Penchev and Antoniya Shalamanova, "A Governance Model for an EU Cyber Security Collaborative Network–ECSCON," *Information & Security: An International Journal* 46, no. 1 (2020): 99-113, https://doi.org/10.11610/isij.4607.

[36] Kristina Ignatova and Dimitar Tsonev, "Integration of Information Resources to Ensure Collaboration in Crisis Management," *Information & Security: An International Journal* 46, no. 2 (2020): 141-152, https://doi.org/10.11610/isij.4610.

[37] European Commission. *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.* Brussels 2020. Accessed 26 March 2021. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive.

[38] William Foote Whyte, *Learning from the Field: A Guide from Experience* (Beverly Hills, CA: Sage Publications, 1984).

[39] Andre Ristaino, "Cybersecurity Critical for System Reliability," InTech – International Society of Automation, May-June 2016, accessed 26 March 26, 2021, https://www.isa.org/intech-home/2016/may-june/features/industrial-automation-cybersecurity-conformity-ass.

[40] Institution of Engineering and Technology, *Code of Practice: Cyber Security and Safety*, 2021, accessed March 20, 2021, https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/.

[41] Hugh Boyes and Roy Isbell, *Code of Practice Cybersecurity for Ships* (London: Institution of Engineering and Technology, 2017), accessed March 20, 2021,

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf.

[42] *Ofgem Competent Authority Guidance*, 2018, accessed March 28, 2021, https://www.ofgem.gov.uk/system/files/docs/2018/11/ofgem_ca_guidance_for_dge_gb_v1.0_final.pdf.

[43] Institution of Engineering and Technology, "Code of Practice: Cyber Security and Safety."

[44] Ing-Long Wu, Cheng-Hung Chuang, and Chien-Hua Hsu, "Information Sharing and Collaborative Behaviours in Enabling Supply Chain Performance: A Social Exchange Perspective," *International Journal of Production Economics* 148 (2014): 122-132, https://doi.org/10.1016/j.ijpe.2013.09.016.

[45] Lisa M. Ellram, "International Purchasing Alliances: An Empirical Study," *The International Journal of Logistics Management* 3, no. 1 (1992): 23-36, https://doi.org/10.1108/09574099210804787.

[46] Nina Shin and Sangwook Park, "Supply Chain Leadership Driven Strategic Resilience Capabilities Management: A Leader-Member Exchange Perspective," *Journal of Business Research* 122 (2021): 1-13, https://doi.org/10.1016/j.jbusres.2020.08.056.

[47] Timothy J. Pettit, Keely L. Croxton, and Joseph Fiksel, "The Evolution of Resilience in Supply Chain Management: A Retrospective on Ensuring Supply Chain Resilience," *Journal of Business Logistics* 40, no. 1 (2019): 56-65, https://doi.org/10.1111/jbl.12202.

[48] Claudia Colicchia, Alessandro Creazza, and David A. Menachof, "Managing Cyber and Information Risks in Supply Chains: Insights from an Exploratory Analysis," *Supply Chain Management: An International Journal* 24, no. 2 (2019): 215-240, https://doi.org/10.1108/SCM-09-2017-0289.

[49] Thomas Y. Choi, Kevin J. Dooley, and Manus Rungtusanatham, "Supply Networks and Complex Adaptive Systems: Control Versus Emergence," *Journal of Operations Management* 19, no. 3 (2001): 351-366, https://doi.org/10.1016/S0272-6963(00)00068-1.

[50] Adrian Davis, "Building Cyber-resilience into Supply Chains," *Technology Innovation Management Review* 5, no. 4 (2015): 19-27, http://doi.org/10.22215/timreview/887.

[51] Graham C. Stevens and Mark Johnson, "Integrating the Supply Chain… 25 Years on," *International Journal of Physical Distribution & Logistics Management* 46, no. 1 (2016): 19-42, https://doi.org/10.1108/IJPDLM-07-2015-0175.

[52] Catarina Roseira, Carlos Brito, and Stephan C. Henneberg, "Managing Interdependencies in Supplier Networks," *Industrial Marketing Management* 39, no. 6 (2010): 925-935, https://doi.org/10.1016/j.indmarman.2010.06.012.

[53] Pettit, Croxton, and Fiksel, "The Evolution of Resilience in Supply Chain Management."

[54] Colicchia, Creazza, and Menachof, "Managing Cyber and Information Risks in Supply Chains."

[55] Christopher Keegan, "Cyber Security in the Supply Chain: A Perspective from the Insurance Industry," *Technovation* 7, no. 34 (2014): 380-381, https://doi.org/10.1016/j.technovation.2014.02.002.

[56] National Cyber Security Centre, "The CAF – A Tool for Assessing Cyber Resilience," 2019, accessed March 27, 2021, https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework#use.

[57] UK Department for Digital, Culture, Media & Sport, "Cyber Security Breaches Survey," April 2017, accessed March 27, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf.

[58] UK Department for Digital, Culture, Media & Sport, "The Network and Information Systems Regulation Impact Assessment," April 2018, accessed March 27, 2021, https://www.gov.uk/government/publications/nis-regulations-impact-assessment.

[59] UK DCMS, "Cyber Security Breaches Survey," 2020.

[60] UK DCMS, "Cyber Security Breaches Survey," 2020.

[61] UK DCMS, "Call for Views on Amending the NIS Regulations 2018," Policy Paper. 2020, accessed March 24, 2021, https://www.gov.uk/government/publications/call-for-views-on-proposed-amendments-to-the-network-and-information-systems-regulations/call-for-views-on-amending-the-nis-regulations-2018#draft-legislation.

[62] Tania Wallis and Chris Johnson, "Implementing the NIS Directive, Driving Cybersecurity Improvements for Essential Services," *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, 15-19 June 2020, https://doi.org/10.1109/CyberSA49311.2020.9139641.

[63] IET, *Code of Practice Cyber Security and Safety*, 2021.

[64] EuroControl, "ATM Cybersecurity Maturity Model," 2017, accessed February 23, 2021, https://www.eurocontrol.int/publication/atm-cybersecurity-maturity-model.

[65] EuroControl, "ATM Cybersecurity Maturity Model."

[66] Scottish Local Government, "Digital Telecare Security Assessment Scheme," 2021, accessed March 24, 2021, https://telecare.digitaloffice.scot/initiatives/digital-telecare-security-assessment-scheme-55.

[67] Daniel dos Santos, Stanislav Dashevskyi, Jos Wetzels and Amine Amri, "Amnesia:33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices," Forescout Research Labs, 2021, accessed March 15, 2021, https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/.

[68] Stacy Simpson, ed., "Software Integrity Controls. An Assurance-based Approach to Minimizing Risks in the Software Supply Chain," SAFECode, 2010, accessed March 15, 2021, https://safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf.

[69] Robert Walton, "What's in Your Software? Federal Initiative Targets Frequently Overlooked Electric Utility Vulnerabilities," *Utility Dive*, March 10, 2021, accessed March

15, 2021, https://www.utilitydive.com/news/whats-in-your-software-federal-initiative-targets-frequently-overlooked-e/595820/.

[70] NCSC, "Supply Chain Security Guidance," 2018, accessed March 26, 2021, https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security.

[71] Wallis and Johnson, "Implementing the NIS Directive, Driving Cybersecurity Improvements for Essential Services."

About the Authors

Tania **Wallis** is a Research Associate at University of Glasgow. She holds a BEng (Hons) in Electrical and Electronic Engineering from University of Edinburgh and a multi-disciplinary Master of Environment from University of Melbourne. Her research is at the nexus of business, engineering, and public policy interests. She brings a practical perspective from her operational experience in industry and is proactive in supporting cooperative public-private partnerships in cybersecurity across the UK and EU. https://orcid.org/0000-0002-6252-6783

Prof. Chris **Johnson** is Pro Vice Chancellor of Engineering and Physical Science at Queens University Belfast. He is an elected member of the UK Computing Research Executive Committee, and a member of the EPSRC ICT Strategic Advisory Team and holds fellowships from both the Royal Aeronautical Society and the Royal Society of Edinburgh. He has some 300 peer reviewed publications and has held fellowships from NASA and the US Air Force. His research focuses on the development of safety critical systems. Under contract to ENISA, Johnson helped design the reporting systems that implement Article 13a on cyber security in the Telecoms Directive (2009/140/EC), which led towards the development of the NIS Directive. http://orcid.org/0000-0003-3174-9308

Dr. Mohamed **Khamis** is a lecturer at the University of Glasgow where he leads research in human-centred security. His team focuses on a) understanding threats to privacy and security that are imposed or facilitated by ubiquitous technologies, and on b) designing user-centred systems that address these threats. His team's research has received funding from the Royal Society of Edinburgh, the EPSRC, and the National Cyber Security Centre. He regularly publishes in CHI, TOCHI and other top HCI and Human-centred security conferences and journals. He has been on the program committee of CHI since 2019 and is an editorial board member for IMWUT and the international Journal of Human-computer studies. Mohamed received his PhD from Ludwig Maximilian University of Munich (LMU). https://orcid.org/0000-0001-7051-5200