

Beyond “Complacency and Panic”: Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?

Johan David Michels* and Ian Walden**

Queen Mary University of London

☞ keywords to be inserted by the indexer

Abstract

This article examines the safeguarding and information obligations the NIS Directive imposes on operators of essential services (OES). The Directive aims to ensure that such services are protected from disruption by requiring OES to take “appropriate and proportionate” security measures. In this article, we look at what this means in practice, with a focus on air transport services. We argue that OES need to identify, assess, and address the cyber risks they face and that such risk management inevitably entails a level of subjective judgement and difficult trade-offs. Regulators should accordingly accord OES significant discretion. However, this raises the risk that OES will abuse their discretion, particularly by engaging in “paper compliance”. Regulators will need to actively challenge OES to ensure that they exercise this discretion appropriately.

Introduction

Modern critical infrastructure relies on network and information systems. Digitisation brings new functionalities and efficiencies, but also increases risks. The more functions are performed across interconnected systems and devices, the more opportunities for weaknesses in those systems arise and the higher the risk of system failures or malicious attacks (collectively: “cyber risks”). This was tragically illustrated by the recent crashes involving Boeing 737 Max airplanes in Indonesia and Ethiopia. The incidences appear to be linked to a malfunction in an automated anti-stall software system, for which Boeing quickly announced a software fix.¹

After such a major incident, companies typically scramble to respond and mitigate damage. Some may succeed in putting in place lasting security improvements. Yet, there is a danger that other companies will return to a state of complacency. Reports suggest that in 2017, less than a third of the boards of FTSE 350 companies in the UK received comprehensive information on cyber risks.² “We have only two modes:

* Researcher, Cloud Legal Project and Microsoft Cloud Computing Research Centre, both at the Centre for Commercial Law Studies.

** Professor of Information and Communications Law and Director, Centre for Commercial Law Studies.

¹ G. Travis, “How the Boeing 737 Max Disaster Looks to a Software Developer” (2019), *IEEE Spectrum*, <https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-software-developer>; K. Stacey, “Boeing says software fix aims to prevent future crashes” (2019), *Financial Times*, <https://www.ft.com/content/4d1ee454-50a7-11e9-b401-8d9ef1626294> [Both accessed 15 December 2019].

² UK Government, *FTSE 350 Cyber Governance Health Check Report 2017*.

complacency and panic”, US energy secretary James Schlesinger reportedly observed of energy policy in 1977.³ Much the same could arguably be said of cybersecurity policy and practice today.

The Network and Information Systems (NIS) Directive is the first comprehensive piece of EU legislation specifically aimed at improving cybersecurity in relation to the protection of critical national infrastructure (CNI).⁴ It follows a series of EU policy proposals and strategy documents issued since 2001.⁵

The obligations under the NIS Directive can be broadly distinguished into two categories. First, safeguarding obligations require operators of essential services (OES) to implement cybersecurity measures and engage in an ongoing cyber risk management process. Secondly, information obligations require the sharing or disclosure of information, to promote transparency and raise awareness. Together, these obligations aim to break the cycle of “complacency and panic”. The EU has adopted a similar provision in respect of telecommunication⁶ and payment services,⁷ as well as under the General Data Protection Regulation (GDPR)⁸ and the e-Privacy Directive.⁹ This ensures a harmonised approach to cybersecurity, with beneficial consequences in terms of establishing a body of regulatory experience, guidance and legal certainty.

However, this article considers whether the NIS Directive is likely to lead to real improvements in the cybersecurity of essential services in the EU or will, instead, become simply another “paper compliance” process, promoting style over substance. First, we show that, in the absence of regulation, companies are insufficiently incentivised to invest in cybersecurity and share relevant information. The NIS Directive attempts to address this issue by imposing safeguarding and information obligations. However, we argue that the NIS Directive may fail to meet its objectives for two reasons. First, cyber risk management inherently entails subjective judgments and difficult decisions, which means that regulators will need to accord OES a substantial level of discretion under the NIS Directive. This then raises the risk of companies abusing that discretion to continue to pursue their own private interests to the detriment of the public interests in cybersecurity, while doing the bare minimum to show regulators an appearance of compliance with the NIS Directive. Secondly, we argue that some provisions of the NIS Directive, particularly concerning incident notification, are drafted too narrowly to cover all relevant cybersecurity incidents. Finally, we consider what regulators should do to uncover and/or discourage a paper-based compliance approach to the NIS Directive.

The NIS Directive is not directly applicable, but obliges Member States to achieve a certain result.¹⁰ Member States have some room for manoeuvre in the transposition process, to take into account specific national characteristics. For example, under the NIS Directive, Member States:

³ Reported in G. Luft and A. Koren, “The Myth of U.S. Energy Dependence” (15 October 2013), *Foreign Affairs*, http://www.iags.org/Luft_Korin_FA2013.pdf [Accessed 15 December 2019].

⁴ Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.

⁵ Commission, “Network and Information Security: Proposal for A European Policy Approach” COM(2001) 2982; Commission, “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” COM(2009) 149; Joint Communication, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace” JOIN/2013/01.

⁶ Directive 2002/21 art.13(a) on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L108.

⁷ Directive 2015/2366 on payment services in the internal market [2015] OJ L337 arts 95–96.

⁸ Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119 arts 32–33.

⁹ Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201 art.1(1); amended by Directive 2009/136 [2009] OJ L337 arts 3–4.

¹⁰ Article 288 TFEU.

- must identify the OES with an establishment on their territory based on national threshold requirements¹¹;
- may designate operators in other sectors as providing essential services under national law¹²;
- must designate national competent authorities to monitor the application of the Directive¹³; and
- must set effective, proportionate, and dissuasive penalties for infringements of the national provisions that implement the NIS Directive.¹⁴

To illustrate how the NIS Directive has been implemented, this article examines the UK as a case study. The UK was among the first Member States to transpose the NIS Directive in May 2018.¹⁵ The UK Government was one of the pioneers in cybersecurity and CNI policy, setting a UK Cyber Security Strategy in 2009 and establishing a critical infrastructure resilience programme in 2010.¹⁶ The UK's scheduled departure from the EU on 31 October 2019 will raise further complications under the NIS Directive, as discussed below. Further, the article draws mainly on examples from the air transport sector. The authors consider air transport of particular interest, since it is a comparatively high-tech sector with both economic and safety implications and inherent international features. The findings are based in part on interviews the authors conducted with the UK Civil Aviation Authority (CAA) from June 2017 to June 2018.¹⁷

Why regulate the cybersecurity of critical national infrastructure?

Definition of cybersecurity

The NIS Directive defines cybersecurity as,

“the ability ... to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services.”¹⁸

This definition follows the three objectives typically considered to form part of cybersecurity (commonly referred to as CIA):

- **Confidentiality:**
only an authorised user can read the data stored on a computer system;
- **Integrity:**
only an authorised user or mechanism can change the data stored on a computer system;
and

¹¹ NIS Directive art.5(1)–(2).

¹² NIS Directive art.3.

¹³ NIS Directive art.8.

¹⁴ NIS Directive art.21.

¹⁵ The Network and Information Systems Regulations 2018, 2018 No.506 (NIS Regulations).

¹⁶ UK Cabinet Office, “Cyber Security Strategy of the United Kingdom: safety security and resilience in cyber space” (2009); UK Cabinet Office, “Sector Resilience Plan for Critical Infrastructure 2010” (2010).

¹⁷ The authors are grateful to colleagues at the UK Civil Aviation Authority for generously sharing their time, information, and insights. Notes of the interviews are on file with the authors.

¹⁸ NIS Directive art.4(2).

- **Availability:**

authorised users can access the data stored on the computer system on request.¹⁹

The NIS definition adds “authenticity”, meaning the “property that an entity is what it claims to be”.²⁰

Cybersecurity and critical national infrastructure

CNI denotes a range of essential services upon which society depends. There are two main concerns for cybersecurity in CNI provision: (1) the provider will under-invest in cybersecurity, and (2) they will fail to share or disclose information about cybersecurity measures and breaches.

Under-investment

In theory, investment in cybersecurity should be at an “efficient” level if the cost of putting in place prevention or mitigation measures is lower than the costs society would otherwise have suffered from preventable incidents.²¹ The latter costs are a factor of the likelihood of an incident occurring and the expected impact. The Government can attempt to manage this risk by assessing these costs and investing in appropriate countermeasures for its own systems. However, it does not directly control investment in cybersecurity by private entities. Instead, control over and accountability for cybersecurity in CNI are diffused across government and industry actors. Absent regulation, the primary driver for private companies to invest in cybersecurity stems from commercial self-interest and market incentives, with security breaches being costly in terms of reinstating compromised systems, loss of valuable data assets and associated reputational implications.²²

However, private companies will generally only take into account the value of the costs they face themselves, and—to some extent—the costs faced by their customers. They will not take account of the wider costs to society (known as “negative externalities”). For CNI, the external costs of a security breach are likely to be much higher than the costs that the company would suffer itself.²³ Given high negative externalities, companies may not be sufficiently incentivised to prevent or mitigate incidents to an efficient level.²⁴ Moreover, since a significant portion of companies’ costs may be reputational, they might choose to mitigate harm by keeping breaches secret or by investing in public relations, instead of in security. In addition, CNI markets are often highly concentrated.²⁵ In the absence of strong competition, companies might offer a lower level of security than consumers desire.²⁶ On the demand side, consumers will likely have insufficient information about security risks they are exposed to and even less about the appropriate nature of the measures implemented to mitigate such risks.²⁷ This information asymmetry makes it difficult

¹⁹D. Zissis and D. Lekkas, “Addressing Cloud Computing Security Issues” (2012) 28 *Future Generation Computer Systems* 583, 586.

²⁰ENISA, “Incident notification for DSPs in the context of the NIS Directive” (2017), p.20.

²¹R. Baldwin, M. Cave, M. Lodge, *Understanding Regulation*, 2nd edn (Oxford: Oxford University Press, 2012), p.126.

²²L. Grigoriadis, “Cybersecurity Insurance and New EU Cybersecurity and Data Protection Rules” (2017) 38 *Business Law Review* 212.

²³Commission, “Network and Information Security: Proposal for A European Policy Approach” (2001), pp.7, 18.

²⁴C. Veljanovski, “Economic Approaches to Regulation” in R. Baldwin, *Oxford Handbook of Regulation* (Oxford: Oxford University Press, 2010), p.21.

²⁵The level of market concentration will differ per sector and by Member State, depending on various factors including the extent of privatisation.

²⁶Veljanovski, “Economic Approaches to Regulation” in *Oxford Handbook of Regulation* (2010), p.21.

²⁷Veljanovski, “Economic Approaches to Regulation” in *Oxford Handbook of Regulation* (2010), pp.21–22; Baldwin, Cave, and Lodge, *Understanding Regulation* (2012), p.18.

to assess and compare the risks associated with various services and therefore value security.²⁸ As a result, companies are incentivized to focus on offering new features or time to market, rather than greater security.²⁹ All of these factors may lead to sub-optimal levels of investment.

This problem could be addressed, in part, through private law mechanisms. For example, CNI operators could be held liable under the tort of negligence for damages caused by cybersecurity incidents that they should have reasonably foreseen and prevented or mitigated.³⁰ This can force operators to internalize previously external costs, which should increase their investment in cybersecurity to a more efficient level.³¹ However, tort liability may be ineffective in case of widespread, dispersed low-cost harms. Even if the total cost to society is high, each individual's cost may be too low to be worth pursuing in court. Moreover, establishing whether an operator's cybersecurity measures were sufficient to fulfil its duty of care is likely to be a disputed matter, requiring expert evidence and increasing the cost and risks of filing a tortious claim.³² This suggests a need for a public law response through regulatory intervention.

Insufficient information-sharing

A second risk is that information relevant to cybersecurity will be held in silos, instead of being shared among those that need it. On the one hand, the Government is likely to have better information about certain attacks and threats, particularly regarding politically motivated actors or large-scale cybercrime.³³ On the other hand, private companies may have better information about the level of security offered by, and breaches of, their own systems.³⁴ The Government can choose to disclose the information it holds and encourage private-sector information-sharing. Yet, in the absence of regulation, it cannot determine the level of information private companies will choose to share.

Information-sharing is likely to benefit cybersecurity, particularly in relation to known vulnerabilities, digital security measures and past attacks. Admittedly, secrecy can improve the security of physical defences (also called "security by obscurity"). In the physical world, looking for vulnerabilities in defences is costly for attackers as doing so puts them in physical danger.³⁵ However, in cyberspace, attackers can mount repeated attacks on a network at low cost; probing firewalls or scanning computers for open ports without much risk of repercussions. Given repeated low-cost attacks, information-sharing is likely to be a more effective tactic than secrecy in cybersecurity.³⁶ In other contexts, secrecy may improve security (also called "security by obscurity") such as in relation to physical defences. Nonetheless, advocates of open source software argue that revealing system details improves cybersecurity by enabling peer review and patching. Hiding such details harms security: if attackers share information, they can learn about vulnerabilities quickly, while defenders do not know where to patch.³⁷

²⁸ Commission, "Network and Information Security: Proposal for A European Policy Approach" (2001), p.7.

²⁹ Commission, "Network and Information Security: Proposal for A European Policy Approach" (2001), p.18.

³⁰ C. Kimber, "Company Liability for Negligent Data Management in the Digital Age" (2016) 28 *Computer and Telecommunications Law Review* 204, 205.

³¹ Baldwin, Cave, and Lodge, *Understanding Regulation* (2012), pp.126–127.

³² Baldwin, Cave, and Lodge, *Understanding Regulation* (2012), pp.126–127.

³³ M. Dunn Cavelty, "25: Cyber-security" in A. Collins, *Contemporary Security Studies* (Oxford: Oxford University Press, 2012), p.19.

³⁴ Cavelty, "25: Cyber-security" in *Contemporary Security Studies* (2012), p.19.

³⁵ Cavelty, "25: Cyber-security" in *Contemporary Security Studies* (2012), pp.34–36, 42–45.

³⁶ Cavelty, "25: Cyber-security" in *Contemporary Security Studies* (2012), pp.31, 42.

³⁷ P. Swire, "A Model for when Disclosure helps Security: what is Different about Computer and Network Security?" in M. Grady and F. Parisi, *The Law and Economics of Cyber Security*, (Cambridge: Cambridge University Press, 2006), pp.29–30; R. Anderson, "Why information security is hard", Conference ACSAC'01, *IEEE Computer Society* (2001), pp.6–7. For a contrasting view, see D. Miessler, "Secrecy (Obscurity) is a valid security layer" (2019), <https://danielmiessler.com/study/security-by-obscurity/> [Accessed 15 December 2019].

Yet market forces do not necessarily encourage such beneficial information-sharing. Sharing information on past breaches could lead to liability or reputational damage. Airlines may prefer to keep a security breach secret, since negative press coverage could scare customers away from their service.³⁸ Sharing a company's cybersecurity strategy risks revealing commercially sensitive information.³⁹ Setting up effective voluntary private cybersecurity information-sharing has proved problematic in practice. In 2004, the EU established the European Network and Information Security Agency (ENISA) as a centre of expertise to provide guidance and advice on cybersecurity.⁴⁰ In June 2019, the EU updated ENISA's mandate through the EU Cybersecurity Act and renamed the organisation the European Agency for Cybersecurity.⁴¹ The European Agency for Cybersecurity ran a voluntary information sharing programme from 2010 to 2013.⁴² However, the programme's outcomes were reportedly only "partially satisfactory", as it suffered from a lack of participation, high membership turnover and difficulties sharing confidential information.⁴³ In sum, companies' commercial self-interest may lead to information being siloed, instead of shared. This suggests a need for regulatory intervention to promote beneficial forms of information-sharing.

What are the cybersecurity requirements of the NIS Directive?

Definition of "essential services"

In 2008, the EU Directive on European Critical Infrastructure (ECI) entered into force, with the aim of improving the general level of protection of critical infrastructure that could, if disrupted, have cross-border impacts.⁴⁴ The Directive aimed at protection from all types of threats, with a priority given to countering threats from terrorism. It defined ECI as,

"an asset, system or part thereof ... which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact [...] on at least two Member States."⁴⁵

The ECI Directive only addressed the energy and transport sectors. Subsequent expansion to other sectors was promised, with priority given to the ICT sector.⁴⁶

The NIS Directive applies to a broader range of services than the ECI Directive. It identifies two categories of service providers: OES, which are directly responsible for CNI, and digital service providers (DSPs).⁴⁷ The NIS Directive recognises that organisations throughout the EU, including OES, rely on certain digital services and that their disruption could have far-reaching effects on key economic and

³⁸ M. Simson, "Cyber security in aviation: The woman who saw the tsunami coming" (2016), *RunwayGirlNetwork*, <https://runwaygirlnetwork.com/2016/05/26/cyber-security-aviation-woman-saw-tsunami-coming/> [Accessed 16 December 2019].

³⁹ A. Aviram, "Network Responses to Network Threats: The Evolution into Private Cybersecurity Associations" in Grady and Parisi, *The Law and Economics of Cyber Security* (2006), pp.154–155.

⁴⁰ Regulation 460/2004 establishing the European Network and Information Security Agency [2004] OJ L77; Regulation 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation 460/2004 [2013] OJ L165.

⁴¹ Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation 526/2013 [2019] OJ L151 (Cybersecurity Act).

⁴² The European Public + Private Partnership for Resilience or "E3PR".

⁴³ ENISA, "EP3R 2010–2013: Four years of Pan-European Public Private Cooperation" (2014), pp.10, 14–23.

⁴⁴ Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L345 (ECI Directive) Recitals 1–5.

⁴⁵ ECI Directive art.2(a)(b).

⁴⁶ ECI Directive art.3(3), (4).

⁴⁷ NIS Directive, Recital 48.

societal activities.⁴⁸ For instance, OES may rely on cloud services as part of their IT systems. However, DSPs are considered to present less of a risk than OES.⁴⁹ This article focuses on the regulation of OES. DSPs are subject to many of the same substantive obligations, although different rules on jurisdiction and enforcement apply. Regulated OES are public or private entities that meet several criteria, of which the most important are:

- they provide a listed service in one of seven CNI sectors: energy, transport, banking, financial markets, health, drinking water, and digital infrastructure⁵⁰;
- and
- they operate on such a scale that their service is “essential for the maintenance of critical societal and economic activities”.⁵¹ This depends on factors such as: the number of users and other sectors that depend on the service; the potential impact on economic and societal activities or public safety and its geographic spread; and any alternative means for the provision of that service.⁵²

Thus, OES resemble operators of ECI, but their importance is assessed at the national level: there is no requirement that their service could impact more than one Member State. The Directive further identifies types of service providers within each of the sectors. For example, within the sub-sector of air transport, three types of providers are listed: airlines, airports, and air traffic control (ATC) operators.⁵³ Member States are required to identify OES with an establishment on their territory. In the UK, the NIS Regulations provide the following threshold requirements for identifying OES in the air transport sector:

- any airport operator with more than 10 million annual passengers;
- any entity licensed to provide en-route ATC, and the ATC provider at any airport with more than 10 million annual passengers; and
- any airline with more than 30 per cent of the annual passengers at any UK airport with more than 10 million annual passengers, or with more than 10 million total annual passengers across all UK airports.⁵⁴

The CAA has not published a list of OES established in the UK. However, based on publicly available passenger numbers for 2018, seven UK airports will likely be covered by the NIS Regulations’ thresholds: Heathrow (80 million annual passengers), Gatwick (46 million), Manchester (28 million), Stansted (28 million), Luton (17 million), Edinburgh (14 million) and Birmingham (12 million).⁵⁵ The National Air Traffic Services (NATS) provides en route ATC and ATC for four of these seven airports. The German company DFS provides ATC for the remaining two (Gatwick and Edinburgh) through a UK subsidiary, while Birmingham airport has an in-house ATC.⁵⁶ Further, by absolute passenger numbers for 2017,

⁴⁸ NIS Directive, Recital 48 art.4.

⁴⁹ NIS Directive, Recital 49; ENISA, “Incident notification for DSPs in the context of the NIS Directive” (2017), p.9.

⁵⁰ NIS Directive, Annex II; Commission, “Communication—Making the most of NIS” COM(2017) 476, Annex 1, pp.20, 23.

⁵¹ NIS Directive, Recital 20, NIS Regulations art.5(2); rr.1(1), 8.

⁵² NIS Directive art.6.

⁵³ NIS Directive, Annex II.

⁵⁴ NIS Regulations Sch.2 r.4.

⁵⁵ CAA, “Airport data 2018”, Table 1, <https://www.caa.co.uk/Data-and-analysis/UK-aviation-market/Airlines/Datasets/UK-Airline-data/2017/Airline-data-annual-reports-2017/> [Accessed 16 December 2019]. Glasgow Airport (9.6 million) would fall just below the threshold.

⁵⁶ See NATS, “Facts, Stats, and Reports”, <https://www.nats.aero/news/facts-stats-reports/>; DFS Press Release, “DFS Group takes over air traffic control in Edinburgh” (29 March 2018), https://www.dfs.de/dfs_homepage/en/Press


airlines EasyJet (68 million passengers) and British Airways (42 million) would be covered,⁵⁷ as—most likely—would Ryanair, which reportedly provides around one-fifth of flights departing from the UK.⁵⁸

Safeguarding obligations

Under the NIS Directive, Member States must ensure that OES take “appropriate and proportionate technical and organisational measures” with regard to the security of the network and information systems they use in the provision of their services. OES must:

- (i) manage the risks posed to those systems;
- (ii) prevent and minimise the impact of incidents affecting those systems, with a view to ensuring the continuity of their services; and
- (iii) have regard to the state of the art and ensure a level of security appropriate to the risk posed.⁵⁹

The requirement to implement “appropriate and proportionate measures” can be viewed as an example of principles-based meta-regulation. It is principles-based, in that the Directive sets out high-level objectives and values, while OES are left free to devise their own systems to implement the principles in practice.⁶⁰ It is meta-regulation in that it requires OES to develop their own internal, self-regulatory responses to a public problem.⁶¹ The aim is to stimulate self-critical evaluation and self-organisation within companies, who then report to regulators on the strategy they have put in place.⁶²

Given the similarities between the definition of ECI and OES, some operators in the energy and transport sectors may qualify as both, namely if their services impact on multiple Member States. As a result, they would be subject to two concurrent EU Directives with respect to the security of their critical service. Under the ECI Directive, each Member State shall identify operators of ECI on its territory, after discussion with other Member States that may be impacted by disruption. It is difficult for outsiders to determine which operators may be subject to both Directives, since under the ECI Directive, information concerning the designation as ECI shall be classified.⁶³ Fortunately, the main requirements under the two Directives are overlapping and/or complementary, rather than contradictory. At first glance, this principles-based approach differs from the more prescriptive obligations established under the ECI Directive, which require operators of ECI to have an operator security plan (OSP) in place and appoint a Security Liaison Officer (SLO) to function as a point of contact with the relevant Member State authority.⁶⁴ However, the ECI Directive describes an OSP as being similar to what is required under the NIS Directive’s safeguarding obligations, namely as a plan that: (i) identifies important assets; (ii) conducts a risk analysis; and (iii) identifies and selects counter-measures.⁶⁵ The main difference in terms of safeguarding obligations thus appears to be that the ECI Directive requires operators to appoint a SLO.  European Commission has

/Press%20releases/2018/29.03.2018.-%20DFS%20Group%20takes%20over%20air%20traffic%20control%20in%20Edinburgh/ [Both accessed 16 December 2019].

⁵⁷CAA, “Airline data annual reports 2017”, <https://www.caa.co.uk/Data-and-analysis/UK-aviation-market/Airlines/Datasets/UK-Airline-data/2017/Airline-data-annual-reports-2017/> [Accessed 16 December 2019].

⁵⁸O. Smith, “How Ryanair is taking over Europe, one country at a time”, *The Telegraph* (28 March 2018), <https://www.telegraph.co.uk/travel/news/how-ryanair-is-taking-over-the-world/> [Accessed 16 December 2019].

⁵⁹NIS Directive art.14(1)–(2); NIS Regulations r.10(1).

⁶⁰Baldwin, Cave and Lodge, *Understanding Regulation* (2012), p.302.

⁶¹C. Coglianese and E. Mendelson, “Meta-regulation and Self-regulation” in *Oxford Handbook of Regulation* (2010), p.150.

⁶²N. Gunningham, “Enforcement and Compliance Strategies” in *Oxford Handbook of Regulation* (2010), p.135.

⁶³ECI Directive art.4(5). The requirement that a company’s designation as an ECI operator be treated as confidential information seems to adopt a security-by-obscurity approach.

⁶⁴ECI Directive arts 5–6.

⁶⁵ECI Directive art.5, Annex II.

launched an evaluation of the ECI Directive, with a report expected in 2019.⁶⁶ The European Commission should clarify the relationship between the ECI Directive and the NIS Directive in its 2019 report, so as to reduce unnecessary uncertainty around the overlap of the two Directives.

Further, multiple Member States can have jurisdiction over the same operator under the NIS Directive, if it has branch offices in several Member States.⁶⁷ For instance, Ryanair, headquartered in Ireland, is reportedly the biggest airline in seven EU countries and the second biggest in five more.⁶⁸ In such cases, Member States are required to consult each other when identifying the same operator as an OES.⁶⁹

Since the approaches taken in national legislation or by national regulators may differ, there is a risk that companies designated as OES in multiple Member States may need to comply with different legal requirements. This could potentially result in serious complications for OES providing transnational services. For example, Ryanair could face one set of regulations when taking off from Spain, and another when landing in the UK. Admittedly, concurrent national competencies should be a familiar issue for air transport regulators and airlines, since air transport is often inherently international. National regulators need to work together to avoid clashes in how the NIS Directive is implemented and interpreted, for instance through the Cooperation Group established under the NIS Directive.⁷⁰ To some extent, authorities should already be co-operating under the ECI Directive with regard to OES who are also designated as ECI.

Information obligations

The NIS Directive imposes two types of information obligations on companies. The first is reactive: OES must comply with requests from regulators to provide any information necessary to assess the security of their systems, including documented security policies, and to provide evidence of the effective implementation of such policies, including the results of a security audit.⁷¹ The UK Government has assigned competent authorities by sector to regulate OES, so they can apply sector-specific knowledge and expertise.⁷² The Government envisages that regulators will use this power to request information to engage in a pro-active and cooperative process of cybersecurity oversight. Regulators and OES should work together to manage risks, assess threats, and agree countermeasures.⁷³

The second is pro-active: OES must notify the relevant authority of security incidents without undue delay, and under the NIS Regulation, “no later than 72 hours” after they become aware of an incident.⁷⁴ In the UK, OES notify their competent sector authority, who in turn informs the national computer security incident response team (CSIRT) as soon as reasonably practicable.⁷⁵ CSIRTs monitor and respond to incidents and provide early warnings to stakeholders about risks.⁷⁶ UK Government has designated the National Cyber Security Centre (NCSC) of the Government Communications Headquarters (GCHQ)

⁶⁶ Commission, “Evaluation of the 2008 European Critical Infrastructure Protection Directive” (2018), https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1378074_en [Accessed 16 December 2018].

⁶⁷ Commission, “Making the most of NIS” (2017), p.24.

⁶⁸ Smith, “How Ryanair is taking over Europe, one country at a time”, *The Telegraph* (28 March 2018).

⁶⁹ NIS Directive art.5(4); CG Publication 07/2018, “Identification of Operators of Essential Services” (2018).

⁷⁰ NIS Directive art.1(2)(b).

⁷¹ NIS Directive art.15(2); NIS Regulations r.15.

⁷² UK Department for Digital, Culture, Media and Sport (DCMS), “Security of Network and Information Systems”, Public Consultation (2017) p.12.

⁷³ DCMS, “Security of Network and Information Systems” (2017), p.12; Department for Transport (DfT), “Guidance—Implementation of the NIS Directive” (2018), p.19.

⁷⁴ NIS Directive art.14(3); NIS Regulations r.11. There is no equivalent obligation under the ECI Directive.

⁷⁵ NIS Directive art.10(3); NIS Regulations r.11(5)(b).

⁷⁶ Commission, “Making the most of NIS” (2017), p.17.

as the CSIRT.⁷⁷ CSIRTs also share information on incidents internationally: when alerted to an incident that will significantly impact on the continuity of an essential service in another Member State, the CSIRT must inform that Member State.⁷⁸ Below, we consider whether these information obligations will adequately reduce the risk of insufficient information sharing identified above.

Finally, in addition to the above disclosure and notification obligations, which are mandatory and hierarchical (i.e. one-way), the NIS Directive also contains provisions regarding information sharing by Member States directly, which tend to be voluntary and communitarian (i.e. two-way). For instance, the NIS Directive sets up a Cooperation Group where Member States, the European Agency for Cybersecurity, and the Commission can exchange best practices and share experiences, and a network for CSIRTs to exchange information on incidents and associated risks.⁷⁹

Will the NIS Directive requirements improve the cybersecurity of CNI?

Safeguarding obligations

On the one hand, risk management obligations are arguably inherent to cybersecurity, since, short of complete isolation, there can be no absolute security in networked information systems. As a result, cybersecurity by nature entails risk management.⁸⁰ Principles-based regulation appears equally well suited to cybersecurity. It differs from rules-based regulation, where policy-makers mandate that companies put in place specific security measures.⁸¹ Since each organisation's IT architecture presents a unique cybersecurity challenge, even a well-informed policy-maker would not be able to determine which assets should be subject to which security requirements in the abstract.⁸² Principles-based meta-regulation leaves companies free to put in place company-specific measures, based on their understanding of their own operations and IT architecture. Principles-based regulation tends to be more appropriate when problems are highly complex and there are no one-size-fits-all solutions, as with cybersecurity.⁸³

Principles-based regulation also suits the dynamic nature of cybersecurity as both threats and vulnerabilities are in a constant state of flux. Changing weather patterns can give rise to unexpected storms that threaten the physical security of data centres, while political events can give rise to newly motivated threat agents. Further, the complexity of modern systems means there are likely to be many unknown vulnerabilities: the more complex an IT system is, the more bugs it is likely to contain.⁸⁴ New vulnerabilities are regularly reported in academic papers or dedicated online repositories.⁸⁵ Once a vulnerability is known, a vendor will generally try to release a "patch": a software update that removes the vulnerability.⁸⁶ A so-called "zero-day exploit" is a tool, code or action that uses an unknown—and so

⁷⁷ NIS Regulations rr.4–5. GCHQ is an intelligence and security organisation that provides signals intelligence and information assurance to the Government and armed forces.

⁷⁸ NIS Directive art.14(5).

⁷⁹ NIS Directive arts 11–12.

⁸⁰ B. Schneier, *Schneier on Security* (Indianapolis, IN: Wiley Publishing Inc, 2008), Introduction.

⁸¹ F. Massacci, R. Ruprai, M. Collinson and J. Williams, "Economic Impacts of Rules- versus Risk- Based Cybersecurity Regulations for Critical Infrastructure Providers" (2016) 14 *IEEE Security & Privacy* 53.

⁸² Massacci et al., "Economic Impacts of Rules- versus Risk- Based Cybersecurity Regulations for Critical Infrastructure Providers" (2016) 14 *IEEE Security & Privacy* 53, 59.

⁸³ Coglianesi and Mendelson, "Meta-regulation and Self-regulation" in *Oxford Handbook of Regulation* (2010), pp.152, 163.

⁸⁴ Cavelty, "25: Cyber-security" in *Contemporary Security Studies* (2012), p.4.

⁸⁵ E.g. "Common Vulnerabilities and Exposures", <https://cve.mitre.org/> [Accessed 16 December 2019].

⁸⁶ Assuming the vendor still supports the software.

unpatched—vulnerability. It should work on all “unpatched” instances of a software program.⁸⁷ Thus, cybersecurity involves an ongoing game of cat-and-mouse between attackers seeking fresh exploits, software vendors issuing patches, and users “patching” their systems. Under principles-based regulation, companies can implement new measures quickly, since there is no need to await a regulator’s or industry group’s agreement.⁸⁸

However, principles-based regulation under the NIS Directive faces several key challenges. First, it is difficult for even well-informed and well-intentioned OES to conduct effective cyber risk management, which inherently involves an element of subjective judgment. Regulators should accordingly accord them significant discretion. However, some operators may fail to use their discretion in the public interest, instead pursuing their own private interests while trying to project an appearance of compliance. The need to accord companies a level of discretion then complicates enforcement, by making it difficult to prove non-compliance. We develop these points in turn below.

Cyber risk management involves discretion in dealing with uncertainty

The NIS Directive defines a risk as “any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems”.⁸⁹ OES are obliged to put in place “appropriate and proportionate” security measures to manage risks and provide a level of security appropriate to the risk posed.⁹⁰ In effect, this requires OES to engage in risk management: the ongoing process of identifying, assessing, and responding to risk.⁹¹ In computer science, a “vulnerability” is a property of a system that creates the potential for a breach of one or more of the CIA objectives.⁹² A “threat” refers to a set of circumstances that may allow a vulnerability to be exploited.⁹³ Thus, a risk occurs when a threat and a corresponding vulnerability exist, or: risk = vulnerability + threat.⁹⁴ The level of risk is determined by the likelihood of the risk materialising into an event and the severity of the possible impact of such an event. Risk is conventionally measured as the probability of an event occurring x the impact of that event.⁹⁵ In relation to cyber risks, the level of risk is: the probability that a vulnerability will be exploited or lead to failure x the expected damage if this occurs, or: level of risk = (threat + vulnerability) x damage. Further, the requirement to put in place “appropriate” measures means that the measures must effectively address the risk. The reference to proportionality suggests the costs of the security measures should be in proportion to the risk.⁹⁶ The Directive aims to avoid imposing disproportionate financial or administrative burdens on the regulated entities.⁹⁷ This suggests that OES should engage in a cost-benefit risk analysis.⁹⁸ In theory, such cost-benefit risk analyses should drive OES to invest in those measures

⁸⁷ US Government, “Vulnerabilities Equities Policy and Process” (2017), p.11; UK GCHQ, “The Equities Process” (2018).

⁸⁸ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), p.147; DfT, “Guidance—Implementation of the NIS Directive” (2018), p.19.

⁸⁹ NIS Directive art.4(9); NIS Regulations r.1(1), (3).

⁹⁰ NIS Directive art.14; NIS Regulations rr.10, 12.

⁹¹ See National Institute of Standards and Technology (NIST), “NIST Framework for improving critical infrastructure cybersecurity v. 1.1” (2018), p.4.

⁹² R. Anderson, *Security Engineering*, 2nd edn (Indianapolis, IN: Wiley Publishing Inc, 2018), p.15.

⁹³ Caverty, “25: Cyber-security” in *Contemporary Security Studies* (2012), p.5.

⁹⁴ ENISA, “Cloud Computing Benefits, risks and recommendations for information security” (2012), p.13.

⁹⁵ J. Black: “The Role of Risk in Regulatory Processes” in *Oxford Handbook of Regulation* (2010), p.310.

⁹⁶ NIS Cooperation Group, “Reference Document on security measures for Operators of Essential Services”, CG Publication 01/2018, p.9.

⁹⁷ NIS Directive, Recital 58.

⁹⁸ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), p.310; NIS Cooperation Group, “Reference Document on security measures for Operators of Essential Services” (2018), p.10.

which effectively reduce risks to society to an “efficient” level.⁹⁹ Thus, under the NIS Directive, an OES should implement a certain measure if: *the cost of measure < the probability of a threat exploiting a vulnerability x the expected damage*.

There is no settled scientific risk assessment method.¹⁰⁰ The NCSC provides a guide for choosing a suitable risk management approach for UK OES, but does not mandate a methodology.¹⁰¹ A risk management process typically involves three key steps.

Step 1: Identifying cyber risks To identify risks, an OES first needs to draw up a list of the systems it uses to provide its essential services, which we will refer to as “critical systems”.¹⁰² These are the systems it needs to protect under the NIS Directive. The UK Department for Transport (DfT) considers that the critical systems for the air transport sector are those that enable aircraft to land and take-off and passengers to depart and arrive. This includes check-in facilities, departure control, security checks, air navigation, and aircraft operation.¹⁰³ Other systems, such as those used for the provision of shopping areas at airports, would only be covered to the extent they are relevant to the security of critical systems.¹⁰⁴

The OES should then identify cyber risks to its critical systems. To do so, it can look for known vulnerabilities in critical systems. In the air transport sector, some aviation-specific software will have been rigorously tested during its design so as to ensure a low risk of faults under aviation safety regulation.¹⁰⁵ For example, the United States Federal Aviation Authority reportedly assesses the content of software and updates to analyse safety implications beforehand.¹⁰⁶ Yet, following the crashes of two Boeing 737 Max airplanes in 2018 and 2019, some have questioned the efficacy of such testing, in particular when the regulator delegates performance of some of the tests to the manufacturer’s staff.¹⁰⁷ Ultimately, even with prior testing, all software will inevitably contain some faults.¹⁰⁸ To identify vulnerabilities, OES might need to engage external experts, for instance to conduct a penetration test (or “pen test”) on its systems, wherein an outsider attempts to breach the security of a system using the same tools and techniques an attacker might.¹⁰⁹ OES also need to identify the threats that could impact the identified vulnerabilities. The NCSC recommends that OES have a “good understanding of the threat landscape” in order to effectively identify risks.¹¹⁰

Step 2: Assessing cyber risks Once an OES has identified relevant cyber risks, it needs to determine which present the highest risk, as measured by the probability of a threat exploiting a vulnerability and the expected damage. In relation to impact, OES also need to consider any mitigating measures already

⁹⁹ As discussed below, this may require placing a monetary value on human safety, which is difficult and highly contentious.

¹⁰⁰ Black, “The Role of Risk in Regulatory Processes” in *Oxford Handbook of Regulation* (2010), p.315.

¹⁰¹ NCSC, NIS Directive Guidance, “Summary of risk methods and frameworks” (2016).

¹⁰² NIS Directive art.14; DfT, “Guidance—Implementation of the NIS Directive” (2018), p.17.

¹⁰³ DfT, “Guidance—Implementation of the NIS Directive” (2018), p.17.

¹⁰⁴ See NIS Directive, Recital 22.

¹⁰⁵ Independent Enquiry Panel, *NATS System Failure 12 December 2014—Final Report* (2015), pp.5–6.

¹⁰⁶ A. Smith, “Franken-algorithms: the deadly consequences of unpredictable code” (30 August 2018), *The Guardian*, https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger?CMP=tw_t_gu [Accessed 16 December 2019].

¹⁰⁷ E.g. D. Gates, “Flawed analysis, failed oversight: How Boeing, FAA certified the suspect 737 MAX flight control system” (17 March 2019) *Seattle Times*, <https://www.seattletimes.com/business/boeing-aerospace/failed-certification-faa-missed-safety-issues-in-the-737-max-system-implicated-in-the-lion-air-crash/> [Accessed 16 December 2019].


¹⁰⁸ See *NATS Enquiry* (2015), pp.5–6.

¹⁰⁹ NCSC, “Penetration Testing”, <https://www.ncsc.gov.uk/guidance/penetration-testing> [Accessed 16 December 2019].

¹¹⁰ NCSC, “NIS Directive Guidance”, *A2. Risk management*, <https://www.ncsc.gov.uk/guidance/a2-risk-management> [Accessed 16 December 2019].

in place, so as to establish the “net” or “residual” risk to each system. OES may already have in place back-up systems to turn to in case of failure (known as “failover”). For instance, if an airline’s electronic boarding passes system fails, it can failover to paper boarding passes. Similarly, pilots fly with paper navigation charts and flight plans and have back-up instruments on their cockpit displays, in case digital charts or instruments fail.¹¹¹

Step 3: Responding to cyber risks Once an OES has assessed the relevant risks, it must decide how to respond. In general, it can:

-  **accept** the residual risk as falling within its risk tolerance;
- **reduce the risk:**
 either by reducing the likelihood of a threat successfully exploiting a vulnerability (e.g. by improving preventative counter-measures), or by mitigating the resulting damage (e.g. by improving failover options); or
- **avoid the risk:**
 by stopping the activity that is causing the risk.¹¹²

While the above steps sound reasonable in principle, they present significant challenges in practice. It is difficult to identify vulnerabilities in complex systems.

In addition, it is difficult to assess the level of risk posed by each specific vulnerability, since threats can come from a wide range of sources, both intentional or unintentional, as well as internal and external.¹¹³ Moreover, human threat agents vary in terms of their purpose and level of organisation, expertise and resources, ranging from well-funded foreign state security services to disgruntled former employees and hacker-hobbyists.

Secondly, while some risks may be quantifiable by extrapolating from statistics regarding the frequency of past events,¹¹⁴ e.g. the likelihood of a storm of a certain severity, other risks are inherently uncertain and are not susceptible to quantitative assessment.¹¹⁵ For example, the likelihood of a terrorist cyber-attack does not lend itself to a statistical analysis. Instead, it is, as Rumsfeld put it, “a known unknown”.¹¹⁶ Compilation reports on the prevalence of certain types of cyber-attacks can indicate their likelihood. For example, the Verizon *2018 Data Breach Investigations Report* noted that over half of the breaches in 2018 featured hacking and a third included malware, while over three-quarters of breaches were financially motivated, with half being carried out by organised criminal groups.¹¹⁷ Nonetheless, a great deal of risk analysis is ultimately concerned with trying to turn such uncertainties into probabilities.¹¹⁸ Given the above, any cost-benefit risk analysis will inevitably be mired in uncertainty.

¹¹¹ R. Charles, “Op-Ed: Why hacking an airliner isn’t just an app away” (16 April 2014), *RunwayGirlNetwork*, <https://runwaygirlnetwork.com/2014/04/16/oped-why-hacking-an-airliner-isnt-just-an-app-away/> [Accessed 16 December 2019].

¹¹² NIST, “NIST Framework for improving critical infrastructure cybersecurity v. 1.1” (2018), p.4.

¹¹³ Cavelti, “25: Cyber-security” in *Contemporary Security Studies* (2012), p.4.

¹¹⁴ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), pp.86–88.

¹¹⁵ Baldwin, Cave, and Lodge, *Understanding Regulation* (2012), p.310; Black, “The Role of Risk in Regulatory Processes” in *Oxford Handbook of Regulation* (2010), p.310.

¹¹⁶ US Department of Defense, “News Briefing—Secretary Rumsfeld and General Myers” (12 February 2002), <http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636> [Accessed 16 December 2019].

¹¹⁷ Verizon, *2018 Data Breach Investigations Report* (2017), p.5, https://www.verizonenterprise.com/resources/reports/2017_dbir_en_xg.pdf [Accessed 16 December 2019].

¹¹⁸ Black, “The Role of Risk in Regulatory Processes” in *Oxford Handbook of Regulation* (2010), p.314.

Cyber risk management is inherently subjective

Deciding how to respond to a risk entails difficult trade-offs and a level of subjective assessment. There is no objective way to determine how safe is safe enough.¹¹⁹ The NIS Directive defines security as the ability to resist actions that compromise CIA and authenticity “at a given level of confidence”. It does not further define that level of confidence. To counteract the risk of under-investment identified previously, OES should put in place measures appropriate to the risk posed to society by disruption of their services. However, assessing and then valuing the relevant “externalities”, i.e. the damage to society to be avoided from possible security breaches, is not straightforward. OES will need to consider at least the expected economic harm to others from any disruption of their service, but will also need to consider public safety. Quantifying the likelihood that a security breach would lead to harm, and then the likely extent of such harm, is difficult, since it depends on a range of factors, including the intentions of a potential attacker and any mitigation measures already taken by affected third parties. Moreover, to compare like-for-like in a strict cost-benefit risk analysis, an OES would also need to attach a monetary value to the potential costs of a service disruption. Thus, an airline would need to determine the “value” to society of passenger time wasted from cancelled flights. This is likely a contentious issue, with no objective answer. Deciding the monetary value of “public safety” and of injuries to be avoided or lives to be saved would be even more difficult.

The wording of the NIS Directive adds to this uncertainty, owing to a lack of clarity around which risks OES should manage. The NIS Directive focuses on services that are “essential for the maintenance of critical societal and economic activities” and explicitly requires OES to take measures to ensure service continuity.¹²⁰ This indicates that OES should focus on the risk of disrupting wider societal and economic activities and causing economic harm. However, it is less clear whether OES should also focus on managing risks that relate to the safety of persons. This is in contrast to the ECI Directive, which defines “critical infrastructure” as being essential to a range of functions, including “health”, “safety” and “security”, and identifies ECI in part based on a “casualties” criterion.¹²¹

There are several indications that the NIS Directive was also intended to capture such risks. First, it mentions public safety as one of the factors to take into account when determining a “significant disruptive effect”, in the context of identifying OES.¹²² Secondly, the European Commission’s thresholds for incident reporting by DSPs mention creating “a risk to public safety, security, or loss of life” as an independent factor.¹²³ Thirdly, the UK Government’s stated approach to penalties under the NIS Directive provides that “an immediate threat to life” is an important factor in determining the size of fines.¹²⁴ Finally, including risks to safety would accord with the UK’s definition of CNI, which covers “those services whose integrity, if compromised, could result in significant loss of life or casualties”.¹²⁵ Nonetheless, the NIS Directive is not explicit on this point, leaving it unclear whether OES should seek to manage risks that involve a physical threat to persons, without leading to widespread service outages. Regulators need to provide guidance on this point.

¹¹⁹ Black, “The Role of Risk in Regulatory Processes” in *Oxford Handbook of Regulation* (2010), p.321.

¹²⁰ NIS Directive art.14(2).

¹²¹ ECI Directive arts 2(a), 3(2)(a).

¹²² NIS Directive, Recital 27 art.6(1)(c).

¹²³ Commission Implementing Regulation 2018/151 [2015] OJ L38 art.4.

¹²⁴ NIS Regulations r.18(6).

¹²⁵ UK Centre for Protection of National Infrastructure, “Critical national infrastructure”, <https://www.cjni.gov.uk/critical-national-infrastructure-0> [Accessed 16 December 2019].

OES should be accorded a level of discretion

In light of the above, any quantitative cyber cost-benefit risk analysis inherently involves an amount of “educated guesswork”, subjective judgements, and difficult trade-offs. When it comes to assessing uncertainties and weighing proportionate responses, there are no objectively right and wrong answers. At most, a cost-benefit risk analysis may help OES rationalise and prioritise their cybersecurity investments.¹²⁶ Such analysis should, at least, point to “obvious” cases, such as where a low-cost measure can reduce a high-likelihood, high-impact risk.

As a result, regulators should arguably give OES a significant measure of discretion under the NIS Directive. As long as an OES follows a defined risk management process, analyses relevant information, and makes a good-faith determination on how to respond, then it will seemingly have complied with the NIS Directive. In this respect, the requirements are more about process than exact outcomes.

Thus, not every security breach—no matter how disruptive—should constitute a breach of the NIS Directive. Provided an OES has conducted a thorough risk management process, it will have discharged its duty. If it subsequently experiences a security breach despite its best efforts, this would not constitute a breach of the NIS Directive. Conversely, an OES could be in breach of its legal requirements, even without a disruptive security breach, if it has failed to undertake diligent efforts to identify risks to its systems. For example, if it has failed to perform a thorough assessment of the risks it faces based on the best available information; or to respond to those risks in an appropriate and proportionate manner. For example, running old, unpatched versions of software on critical systems could indicate a failure to identify obvious risks—if the OES was unaware—or to respond adequately if the OES identified the vulnerability, but failed to take appropriate action within a reasonable time.

OES may abuse their discretion

With principles-based meta-regulation, the regulator operates at a distance: it relies on companies to put in place appropriate systems and acts only to ensure that these mechanisms are working effectively.¹²⁷ Companies should in the first instance translate high-level principles into practice. Doing so typically involves a good deal of judgement.¹²⁸ Given the extent of discretion in interpreting principles-based meta-regulation, it can be difficult to determine definitively that the regulation has been breached. This highlights a primary problem with principles-based meta-regulation: although companies have better access to information about their own cybersecurity, they do not necessarily have the right incentives to use that information to further the public interest. Thus, the challenge is to ensure that companies use the discretion they are granted under meta-regulation in ways consistent with the regulation’s objectives, rather than their own private interests.¹²⁹

In the context of the NIS Directive, this refers to OES fully considering the wider damages to society from the possible disruption of their services as part of their cyber risk management, not only the damages to their own commercial interests (to the extent that they diverge). In theory, the NIS Directive should drive OES to internalise negative externalities, so as to reduce the risk of under-investment, as set out above. However, in practice, companies differ both in terms of their ability and their motivation to comply. While low-capability companies lack the required information or expertise to implement appropriate measures; ill-intentioned companies will simply not be inclined to do so. Indeed, an ill-intentioned company may take a risk-based approach to compliance: weighing up the benefit of

¹²⁶ See Black, “The Role of Risk in Regulatory Processes” in *Oxford Handbook of Regulation*, (2010), p.322.

¹²⁷ Gunningham, “Enforcement and Compliance Strategies” in *Oxford Handbook of Regulation* (2010), p.135.

¹²⁸ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), p.304.

¹²⁹ Coglianese and Mendelson, “Meta-regulation and Self-regulation” in *Oxford Handbook of Regulation* (2010), p.153.

non-compliance in terms of business opportunities against the cost of potential sanctions. This could lead the company to approach compliance as a periodic negotiation with the regulator and only put in place those measures the regulator requests to review.¹³⁰ Wherever possible, the company will translate the high-level principles into practices that accord with its own objectives, mainly of pursuing profits.¹³¹ As a result, it may pursue an approach of “paper compliance” with the NIS Directive,¹³² while avoiding having to invest in costly cybersecurity measures. This may even enable them to undercut more-compliant competitors.

The problem is that since regulators should accord OES a level of discretion under the NIS Directive, it is difficult to assess which companies are really investing in improved security, and which are merely engaging in security window-dressing. For example, an OES may report that it is training its staff on best practices for countering social engineering and phishing attacks. How can a regulator assess whether that training is in fact being implemented across the organisation, and if so, whether the training will effectively prevent staff from clicking on links in phishing emails? Similarly, it is difficult for a regulator to assess whether a patch management plan is deployed consistently across a company.

Unlike the Data Protection Officer (DPO) requirement under the GDPR, the NIS Directive does not require OES to appoint an independent security officer with sufficient resources to monitor and advise on compliance.¹³³ The DPO function effectively internalises an element of independent supervision within companies to provide a first level of regulatory scrutiny. When effective, this can help reduce the regulator’s burden, although traditional concerns around “regulatory capture” of the DPO remain.¹³⁴ Further, while the ECI Directive does require operators of ECI to appoint an SLO, it does not require the SLO to be independent or have sufficient resources. Instead, the SLO’s task under the ECI Directive relates primarily to exchanging relevant information concerning identified risks and threats with Member State authorities.¹³⁵ As a result, there is no requirement for an independent, internal expert to challenge an OES’s decisions on security.

In addition, unlike the accountability principle under the GDPR, there is no explicit requirement under the NIS Directive for companies to pro-actively demonstrate their compliance on an ongoing basis.¹³⁶ Nor does the NIS Directive require an OES to have a documented operator security plan in place, in contrast to the ECI Directive.¹³⁷ While these reduced documentary requirements may mitigate against “paper compliance” by regulatees, it may also encourage some companies to take a reactive approach and focus their compliance programmes on responding to requests from regulators.¹³⁸ To some extent, regulators can try to counter “paper compliance” approaches by appointing or requiring companies to appoint external security experts to conduct pen tests on certain systems. Under the NIS Regulations, a regulator can conduct an inspection of an OES itself, or appoint a person to conduct an inspection on its behalf.¹³⁹ However, pen tests only provide a partial answer. They identify vulnerabilities open to potential deliberate threats, but would not necessarily identify those subject to accidental threats. Moreover, a pen test is only as effective as the pen tester and the test case library they deploy.¹⁴⁰ Finally, a pen test is a point-in-time

¹³⁰ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), pp.150–153.

¹³¹ Baldwin, Cave, and Lodge, *Understanding Regulation* (2012), p.309.

¹³² Gunningham, “Enforcement and Compliance Strategies” in *Oxford Handbook of Regulation* (2010), p.138.

¹³³ Cf. GDPR arts 38–39.

¹³⁴ See C. Quelle, “Privacy, Proceduralism and Self-Regulation in Data Protection Law” (2017) 1 *Teoria Critica della Regolazione Sociale* 105.

¹³⁵ ECI Directive art.6(4).

¹³⁶ Cf. GDPR art.5(2).

¹³⁷ ECI Directive arts 5–6.

¹³⁸ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), pp.150–153.

¹³⁹ NIS Regulations r.16.

¹⁴⁰ R. Savola, “On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems” (2010) 10 *I.J.C.S.N.S.* 232.

assessment. It does not measure an organisation's ability to maintain or monitor its systems over time. Moreover, such tests are likely too costly to be held regularly on large numbers of systems. As a result, "paper compliance" may not be unveiled until it is too late: namely, when an incident reveals a structural weakness in an OES's security.

Information obligations

Will the information obligations under the NIS Directive help regulators monitor and assess OES compliance and reduce the "paper compliance" risk we have identified? Taken together, the obligations to provide regulators with information on request and to notify regulators of incidents, serve to reduce the risk of information being held in silos. The regulator should be in a position to collect relevant information from across a sector and review OES' strategies side-by-side. It can use this information to establish industry benchmarks, identify best practices, and promote their wider adoption, as well as to spot gaps in a particular OES's strategy. Further, the detection of relevant incidents is key to understanding companies' level of compliance and the effectiveness of the regime.¹⁴¹ Regulators can use information regarding specific incidents to update their understanding of the risks a sector faces, amend their guidelines, and inform their enforcement strategy. Ideally, a regulator will be able to obtain sufficient information from the companies in its sector to determine each company's ability and motivation to comply. It can then tailor and target its responses accordingly.¹⁴² The competent authority or CSIRT can provide an OES with information relating to the incident, in order to assist them in dealing with that incident more effectively or to prevent future incidents.¹⁴³ In this manner, UK OES can benefit from the NCSC's expertise when they report an incident. In addition, the regulator can alert other companies across sectors to a vulnerability or an emerging threat.¹⁴⁴

However, there are limits to this approach. First, sectoral regulators need a solid understanding of cybersecurity in order to know what information to request from OES and how to assess it. In the UK, the Secretary of State for Transport (DfT) and the CAA are the competent authority designated for OES in the air transport sub-sector.¹⁴⁵ While cybersecurity is not a completely new issue for the air transport sector, it is a new area of competence for the CAA, requiring it to obtain the necessary in-house expertise and recast its approach to risk assessment, focusing on security rather than safety.¹⁴⁶

Secondly, the incident notification requirements may be too narrowly drafted to cover all relevant incidents. The NIS Directive defines an "incident" as any event having an actual adverse effect on the security of network and information systems,¹⁴⁷ meaning on the CIA or authenticity of data or related services.¹⁴⁸ Not every incident that breaches CIA or authenticity will qualify as a "significant" incident requiring notification. Instead, the obligation for OES to notify applies to incidents that have a significant impact on the continuity of their essential services.¹⁴⁹ Significance should be determined based on the number of users affected by the disruption; the duration; and the geographic area affected.¹⁵⁰ In the air transport sector, the DfT has set as a threshold for notification a single incident that, within a 24-hour period, results in:

¹⁴¹ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), p.272.

¹⁴² Baldwin, Cave and Lodge, *Understanding Regulation* (2012), p.262.

¹⁴³ NIS Regulations r.11(7).

¹⁴⁴ See R. Anderson, R. Böhme, R. Clayton and T. Moore, "Security Economics and European Policy", ISSE 2008 Securing Electronic Business Processes (2009), pp.77–80.

¹⁴⁵ NIS Regulations r.3(1) and Sch.1.

¹⁴⁶ Interview with the CAA, notes on file with the authors, 27 October 2017.

¹⁴⁷ NIS Directive art.4(7).

¹⁴⁸ Commission, "Making the most of NIS" (2017), p.31.

¹⁴⁹ NIS Directive art.14(3); NIS Regulations r.11(1).

¹⁵⁰ NIS Directive art.14(4); NIS Regulations r.11(2).

- **for major airports:**
more than 20 per cent of scheduled flights being cancelled;
- **for ATC providers:**
more than 10,000 unscheduled, en-route delay minutes;
- **for airlines:**
more than 30 per cent of the scheduled flights across the UK being cancelled.¹⁵¹

Setting specific metrics for notification thresholds provides legal certainty. However, the metrics may be too narrow in two respects. First, notification is required only for security breaches that disrupt an essential or digital service. This reflects the Directive’s aim to ensure CNI continuity. Yet there can be far-reaching security breaches of OES systems that do not lead to significant disruption. For instance, an attacker could gain unauthorised access to the system and obtain root privileges, without causing mass disruption. For example, a security researcher reportedly told the FBI that he had hacked into aircrafts’ in-flight networks more than a dozen times in the period 2011 to 2014, through the in-flight entertainment system. To do so, he connected his laptop to the seat electronic box and used default IDs and passwords to gain access to the aircraft’s systems, including the thrust control systems.¹⁵² While this incident indicated serious security vulnerabilities, it did not lead to any delays and so would not trigger a notification requirement. Similarly, if an OES suffered a ransomware attack, but paid the ransom before it caused any disruption to its service, this would not trigger a notification requirement. As a result, regulators may need to regularly ask OES for information about non-notifiable breaches, in order to identify emerging security trends.

Further, there could be widespread breaches of confidentiality which do not (directly) affect the continuity of services. For example, on 6 September 2018, British Airways announced that it had suffered a breach of the names, email addresses, and credit card information of around 380,000 customers.¹⁵³ Subsequent reports indicated that the attackers had access to British Airways servers, since they were able to modify the website’s code.¹⁵⁴ Although this incident looked like a serious security breach, it did not result in delays or cancellations of flights. Such incidents might highlight significant vulnerabilities in an OES’ security, but would not trigger a notification obligation.¹⁵⁵ As a result, regulators may not be notified of important vulnerabilities and will not be able to warn other operators. Nonetheless, in cases involving personal data, such breaches would be subject to a notification requirement under the GDPR. British Airways notified the 2018 breach to the Information Commissioner’s Office (ICO), which has opened an investigation.¹⁵⁶ Thus, NIS Directive authorities may need to regularly liaise with national data protection authorities to identify emerging security trends.

Secondly, notification thresholds may fail to capture all relevant risks. For example, the DfT’s thresholds for air transport OES do not require notification for incidents that create a risk to public safety, security,

¹⁵¹ DfT, “Guidance—Implementation of the NIS Directive” (2018), Annex E, p.44.

¹⁵² K. Zetter, “Feds Say that Banned Researcher Commandeered a Plane” (2015), *Wired*, <https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/> [Accessed 16 December 2019].

¹⁵³ British Airways, “Customer Data Theft” (2018), <https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information> [Accessed 16 December 2019].

¹⁵⁴ RISKIQ, “Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims” (11 September 2018), <https://www.riskiq.com/blog/labs/magecart-british-airways-breach/> [Accessed 16 December 2019].

¹⁵⁵ ENISA, “Incident notification for DSPs in the context of the NIS Directive” (2017), p.20.

¹⁵⁶ ICO, “Statement update in response to British Airways breach” (25 October 2018), <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/ico-statement-in-response-to-british-airways-breach-announcement/> [Accessed 16 December 2019].

or loss of life. As a result, if a security breach were to endanger the passengers and crew, but not result in mass delays, it would not trigger a notification requirement under the DfT's NIS Directive thresholds. This may, in part, stem from the lack of clarity around which risks OES should manage under the NIS Directive, as discussed above. In theory, this suggests that incidents like the two Boeing 737 Max crashes would only be notified to the UK regulator if they caused further service disruption. Regulators need to clarify this important point, or risk missing information on safety-related incidents.



How should regulators enforce the NIS Directive?

Guidance and collaboration

To counteract the challenges of uncertainty under the NIS Directive identified above, regulators can issue guidance on how to interpret and implement the Directive. For example, the NIS Cooperation Group has published a series of guidelines and reference documents under the NIS Directive.¹⁵⁷ In the UK, the NCSC has set out high level security principles, which are complemented by sector-specific guidelines from competent authorities.¹⁵⁸ It has also developed a framework for OES to perform a cybersecurity self-assessment, with a list of indicators of “good practice”.¹⁵⁹ Sectoral regulators have also prepared and published guidance on NIS implementation.¹⁶⁰ The CAA has developed an air-transport-sector-specific cyber assessment framework known as “CAP 1574”, with a self-assessment tool, known as the “CAF”.¹⁶¹ CAP1574 sets out 26 security controls as a framework for managing cyber risks in aviation. It references international standards, such as ISO and NIST standards as examples.¹⁶² The framework aims at supporting both safety requirements and economic resilience.¹⁶³

Admittedly, the more detailed guidance regulators provide, the more a principles-based regime begins to resemble rules-based regulation.¹⁶⁴ Nonetheless, OES remain free to adopt alternate methods of demonstrating compliance. For example, under the NIS Directive, an OES can seek to comply by following European Agency for Cybersecurity guidance and industry standards strictly, or by achieving an equivalent level of cybersecurity using alternate measures. In addition, regulators can more easily adjust their guidance to reflect new technological developments, than legislators can re-write prescriptive rules.¹⁶⁵

Monitoring compliance

To counteract the risk of OES engaging in mere “paper compliance”, regulators must take a pro-active approach to monitoring OES’ security practices. Regulators need to actively challenge companies to demonstrate that their systems work in practice, scrutinise their measures, and judge if the company has the leadership, staff, systems, and procedures in place to meet its obligations.¹⁶⁶ For example, the CAA

¹⁵⁷ European Commission, “NIS Cooperation Group”, <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group> [Accessed 16 December 2019].

¹⁵⁸ DCMS, “Security of Network and Information Systems” (2017) p.15; NCSC, “Guidance on NIS Directive Objectives”, <https://www.ncsc.gov.uk/guidance/nis-directive-top-level-objectives> [Accessed 16 December 2019].

¹⁵⁹ NCSC, “NIS Directive—Cyber Assessment Framework”, <https://www.ncsc.gov.uk/guidance/indicators-good-practice> [Accessed 16 December 2019].

¹⁶⁰ NIS Regulations r.3(3); DfT, “Guidance—Implementation of the NIS Directive” (2018).

¹⁶¹ DfT, “Guidance—Implementation of the NIS Directive” (2018), pp.19, 25.

¹⁶² CAA, “CAP1574: Twenty-six security controls for regulation”, <http://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=8111>.

¹⁶³ DfT, “Guidance—Implementation of the NIS Directive” (2018), p.24.

¹⁶⁴ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), p.307.

¹⁶⁵ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), p.310.

¹⁶⁶ Gunningham, “Enforcement and Compliance Strategies” in *Oxford Handbook of Regulation* (2010), p.135.

has stated that it requested each OES in the air transport sub-sector to perform a self-assessment by the end of 2018. The CAA will then discuss the results with each OES and determine any necessary improvements. If required, the CAA may instruct the OES to appoint an independent third party to conduct audits or testing.¹⁶⁷

Nonetheless, active engagement and scrutiny are resource-intensive and security experts are a finite resource. This raises the question: how should regulators direct their resources to monitor and challenge OES? One answer would be for regulators to adopt a risk-based approach to enforcement: focusing their efforts on those companies that pose the biggest threat to the interests protected by the NIS Directive.¹⁶⁸ To this end, a regulator would first need to analyse which OES pose the biggest “inherent” risk of disrupting societal and economic activities.¹⁶⁹ In the air transport sector, it could be argued that ATC providers pose a greater inherent risk than airlines, since multiple airlines may rely on a particular ATC provider. Then, the regulator would need to consider the “management risk” of each company, namely the company’s own ability and motivation to effectively manage and reduce the risk they pose.¹⁷⁰ This would allow the regulator to identify those companies that pose the highest “net risk” and prioritise those in its monitoring. For example, the CAA plans to use the results of companies’ 2018 self-assessments and combine them with its own threat and vulnerability information to establish a risk-based programme of ongoing monitoring. It will then focus on those companies where the most serious concerns have been identified and/or where potential incidents could have the greatest impacts.¹⁷¹

However, there are problems with such a risk-based approach to enforcement. First, it assumes that the company is the right level for assessing risks. As a result, regulators may miss systemic risks that apply across the industry.¹⁷² For example, were all airlines to rely on the same cloud computing infrastructure provider, then a single vulnerability could create an industry-wide risk. Further, companies are often part of corporate groups subject to parent company control (e.g. British Airways is owned by International Airlines Group, which also owns Aer Lingus, Iberia, and Vueling), such that airlines designated as OES may share corporate systems with other airlines who are not designated as OES or, indeed, businesses unrelated to the air transport industry, potentially giving rise to security vulnerabilities. Alternatively, cybersecurity across the corporate group may benefit from the enhanced demands made of OES airlines in respect of shared systems.

Risk-based enforcement further requires a regulator to make difficult judgment calls as to the motivation and ability of different companies. There are no clear metrics for motivation, requiring regulators to make subjective assessments. The regulator may misjudge these factors, overestimating the effectiveness of a measure a company has put in place to prevent or mitigate damage from a particular type of risk. In that case, the risk will continue to exist, since it is incorrectly deemed a low “net risk”. Although audits could expose such hidden risks, regulators are less likely to submit systems they consider a low net risk to such a high-cost assurance method.

A supplementary approach would be for regulators to develop technical means of cybersecurity assurance as a form of “RegTech”—i.e. the adoption of technologies to facilitate the delivery of regulatory requirements. Thus, software could be used to automatically scans systems for known vulnerabilities and report the results back to OES and regulators. For example, companies such as SecurityScorecard and Upguard provide cybersecurity ratings for companies based on publicly accessible data like traffic to and from the company. Upguard claims to base its ratings on scans of “misconfigurations”, by looking at a

¹⁶⁷ DfT, “Guidance—Implementation of the NIS Directive” (2018), pp.20, 26–27.

¹⁶⁸ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), pp.281–282.

¹⁶⁹ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), pp.281–282.

¹⁷⁰ Baldwin, Cave and Lodge, *Understanding Regulation* (2012), p.304.

¹⁷¹ DfT, “Guidance—Implementation of the NIS Directive” (2018), p.20.

¹⁷² Baldwin, Cave, and Lodge, *Understanding Regulation* (2012), pp.281–282.

company's online "footprint" and determining how that compares to best practices.¹⁷³ This could help regulators spot hidden risks that OES had overlooked during their own risk management.

Sanctions

Finally, the regulator can impose sanctions under the NIS Directive when appropriate risk management measures were not in place without good reason.¹⁷⁴ The threat of sanctions should have a deterrent effect. For instance, a well-intentioned but underfunded IT department could use the risk of sanctions to convince a disinterested, cost-focussed board to give it the budget it needs for additional security measures.

Under the NIS Directive, Member States must lay down rules on penalties for breaches that are effective, proportionate, and dissuasive.¹⁷⁵ In the UK, the regulator can issue a penalty up to a total of £17 million.¹⁷⁶ The highest penalties are reserved for incidents resulting in an immediate threat to life or significant adverse impact on the UK economy.¹⁷⁷ The Government had initially proposed higher penalties, namely at 2 per cent of global turnover for lesser offences or 4 per cent of global turnover for more serious offences, to match the GDPR.¹⁷⁸ However, following objections during its consultation, the Government reduced the penalties.¹⁷⁹ The OES can challenge the penalty decision, including the grounds for imposing the penalty and its sum, and request that the regulator appoint an independent person to review the decision.¹⁸⁰ Further appeals can be brought before the courts.

Finally, regulatory enforcement under the NIS Directive is not the only legal incentive for companies to improve their cybersecurity. The GDPR would also apply where a cybersecurity breach involves personal data. Companies may also be exposed to private law remedies, under contract or tort, for a failure to put in place adequate cybersecurity measures. Indeed, public laws like the NIS Directive may facilitate private law actions by identifying standards of care to which companies can be held accountable.¹⁸¹

Brexit

As of the time of writing, the UK is scheduled to leave the EU on 31 January 2020. The UK Government stated its intention that NIS Regulations will continue to apply in the UK after Brexit.¹⁸² However, it is unclear how Brexit will affect the UK's ability to co-ordinate with Member States in relation to cybersecurity. For example, it is unlikely that the UK can remain a member of the European Agency for Cybersecurity after Brexit.¹⁸³ As noted above, the European Agency for Cybersecurity plays an important role under the NIS Directive by providing guidelines for compliance and sharing best practices, including through the NIS Coordination Group. It further provides the secretariat for the network of national CSIRTS established under the NIS Directive.¹⁸⁴ Third countries can participate in the European Agency for

¹⁷³ Upguard, "BitSight vs SecurityScorecard" (5 December 2019), <https://www.upguard.com/articles/bitsight-vs-securityscorecard> [Accessed 16 December 2019].

¹⁷⁴ DCMS, "Security of Network and Information Systems" (2017), p.25.

¹⁷⁵ NIS Directive art.21.

¹⁷⁶ NIS Regulations r.18(1) and (2).

¹⁷⁷ NIS Regulations r.18(6).

¹⁷⁸ DCMS, "Security of Network and Information Systems" (2017), p.25.

¹⁷⁹ DCMS, "Security of Network and Information Systems" (2017), p.16.

¹⁸⁰ NIS Regulations r.19.

¹⁸¹ In the UK, such actions have been legislated for in respect of competition law breaches: see Competition Act 1998 s.47A.

¹⁸² DCMS, "Security of Network and Information Systems" (2017), p.7.

¹⁸³ See e.g. House of Parliament Commons Select Committee European Scrutiny, "Digital Single Market: ENISA/EU Cybersecurity Agency Regulation" (2017), <https://publications.parliament.uk/pa/cm201719/cmselect/cmeuleg/301-iv/30105.htm> [Accessed 16 December 2019].

¹⁸⁴ NIS Directive art.12(2).

Cybersecurity with approval from the Commission.¹⁸⁵ As of July 2019, the Agency had three third-country representatives as non-voting observers: Iceland, Liechtenstein, and Norway.¹⁸⁶

The UK Government has stated that if it cannot remain a member of the European Agency for Cybersecurity or the CSIRT network, it will instead rely on bilateral relationships to share expertise and information.¹⁸⁷ Further, in July 2019, the UK Government proposed to amend NIS Regulations post-Brexit. However, the proposal focused only on ensuring that digital service providers established outside of the UK would nominate a representative in the UK.¹⁸⁸ It did not address the UK's co-operation with Member States. That same month, British diplomats were reportedly disinvented from an EU meeting on cybersecurity standards,¹⁸⁹ which may prove a troubling sign of things to come.

Concluding remarks

Above, we have identified two main risks in relation to the cybersecurity of companies that manage CNI. First, absent regulation, companies that manage CNI are likely to underinvest in cybersecurity measures, by failing to take full account of wider damages to society. Secondly, they may fail to share information that could help other companies identify vulnerabilities and spread best practices. Poor cybersecurity can result in service disruption, with significant socio-economic impacts. To counter this risk, the NIS Directive requires Member States to impose safeguarding and information obligations on OES.

Safeguarding obligations aim to make the OES take account of the possible negative externalities to society that may stem from disruptions of their service. Since what is “appropriate” and “proportionate” will differ per company and over time, OES need to engage in an ongoing cyber risk management process. This necessarily entails some level of subjective judgement and trade-offs between safeguards, cost and convenience. Regulators therefore need to accord companies a significant measure of discretion in implementation. They will have breached their obligations only when they have demonstrably failed to take reasonably required efforts to identify, assess or address cyber risks.

The NIS Directive's risk-based approach could be undermined in two ways. First, some OES may abuse this discretion by only putting in place those security measures they consider to serve their own commercial interests. OES may try to mask this approach by creating whatever security documentation the regulator asks to see, without meaningfully changing their approach. The result could be a “paper compliance” approach, involving lots of cybersecurity documentation, but insufficient actual cybersecurity. Such approaches may only be unveiled when it is too late, i.e. when the company suffers a cybersecurity incident. In that case, the NIS Directive will have failed to move CNI operators beyond the current cycle of “complacency and panic”, but instead lead only to complacency masquerading as compliance.

Companies abusing their discretion is a general issue for principles-based regulation, but is of heightened concern when regulating the conduct of CNI operators. Unlike the GDPR, there is no requirement to appoint an internal expert with sufficient resources and independence to monitor and advise on compliance, who could challenge an OES's security decisions. As a result, the NIS Directive relies heavily on regulators being able to discourage paper compliance. It gives regulators the relevant tools do so, by requiring

¹⁸⁵ Cybersecurity Act art.42.

¹⁸⁶ ENISA, “List of ENISA Management Board Representatives and Alternates” (2019), <https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/MBMemberAlternate.pdf> [Accessed 16 December 2019].

¹⁸⁷ DCMS, Letter to the Chair of the European Scrutiny Committee TO2018/07325/DC (2018), [http://europeanmemoranda.cabinetoffice.gov.uk/files/2018/05/eCase_07325_-_Cash_\(1\).pdf](http://europeanmemoranda.cabinetoffice.gov.uk/files/2018/05/eCase_07325_-_Cash_(1).pdf) [Accessed 16 December 2019].

¹⁸⁸ DCMS, “Security of Network and Information Systems, Government proposed approach to regulating non-UK based digital service providers” (2019).

¹⁸⁹ M. Khan, “UK shut out of EU key cyber security meeting” (2019), *Financial Times*, <https://www.ft.com/content/e9865874-aa41-11e9-b6ee-3cdf3174eb89> [Accessed 16 December 2019].

companies to disclose security information and notify incidents. Regulators need to use these tools pro-actively to scrutinise and challenge OES' risk management decisions. However, to do so effectively, regulators will need to obtain in-house expertise on cybersecurity. Further, incident notification thresholds that focus on levels of disruption may result in "near-misses" or other non-disruptive but systemic security breaches going unreported. Thus, regulators may need to ask OES for information on non-notifiable security breaches and liaise with data protection or other authorities. Regulators should also clarify some of the identified uncertainties through guidance, including the relationship between the ECI Directive and the NIS Directive, and whether OES are required to focus only on risks of socio-economic impacts under the NIS Directive, or should also seek to manage risks relating to safety, like loss of life. Moreover, regulators should be mindful of clashes in national approaches, particularly where OES face the possibility of being concurrently subject to multiple, differing sets of national rules.

Secondly, in case of a major cybersecurity breach, regulators will inevitably face considerable political pressure to make rapid decisions, finger-point and impose punitive sanctions. There is a risk that this will lead to scapegoating, ignoring the subtleties of the risk-based approach set out in the NIS Directive. This could, in turn, result in legal appeals of decisions that the regulator may find difficult to defend. In sum, while the NIS Directive serves an admirable policy goal, it remains to be seen whether it will actually improve the cybersecurity of Europe's critical national infrastructure.