Cetome
Securing a Better Future

White Paper

INTRODUCTION TO THE NIS DIRECTIVE

April 2019

Author: Dr. Cédric LEVY-BENCHETON, CEO

Table of Content

INTRODUCTION

The Directive on security of network and information systems (NIS Directive) is one major cyber security regulation in these recent years. The objective of the NIS Directive is to strengthen the protection of the services we use in our daily lives against cyber attacks. This includes Operators of Essential Services (including several Critical National Infrastructure operators) and Digital Service Providers.

In this article, we will learn more about the NIS Directive, the scope of application and its obligations. More articles will follow in this series to better apprehend this directive.

WHY THE NIS DIRECTIVE?

The convergence to IP-connected systems is here. We live in a connected world and use interdependent cyber-physical systems every day. These cyber-physical systems rely on software and networks to provide a service in the physical world. To add to this complexity, human operators use computer systems for remote command/control these systems.

Cyber-physical systems face several security risks: vendors and integrators are not security experts. Moreover, several cyber-physical systems are “legacy systems” that were designed before IP-connectivity. They were not meant to be connected and may not be supported by their vendors.

Yet, connectivity brings very interesting functionalities to optimise operations and maintenance, leading these systems to become interdependent. As such, they also face traditional cyber security risks such as malware, ransomware or Denial of Service.

Hence, cyber security is important to prevent issues that could impede safety, our economy or our society. For all these reasons, the NIS Directive was created to better prepare against these cyber risks.

THE CONSEQUENCES OF A CYBER ATTACK

Since Wannacry happened in May 2017, nobody will argue that our society is safe from cyber attacks. In the United Kingdom, the National Health Service was severely impacted and thousands of patients have seen their appointment cancelled. In Germany, train stations and passenger information systems malfunctioned. Yet, it was very lucky that Wannacry did not cause any casualty!

Wannacry was a wake-up call for several organisations that were hit by this ransomware: they were not a target and this was far from a sophisticated attack (it was easy to remediate even when patching was impossible).

Before and since then, several other attacks have been happening, with similar impacts but barely the same degree of visibility in the media. These cyber attacks cause direct damage to our society, with service disruption and data loss that could impede our privacy. They also lead to organisational risks with users losing trust in the organisations hit, as well as potential breaches in regulation. Moreover, some cyber attacks have significant consequences on our society, with an economic impact and potential human casualties.

THE NIS DIRECTIVE OR THE “GDPR OF CRITICAL INFRASTRUCTURE”

The NIS Directive is a European Union Directive, meaning “a legal act of the European Union which requires member states to achieve a particular result without dictating the means of achieving that result”. As such, the NIS Directive requires a local implementation by its 27 Member States as well as in the United Kingdom under the name “NIS Regulations”.

The NIS Directive formalises the requirements for the security of network and information systems to enhance the protection against incidents that could disrupt systems or data contributing to a service.

Developed at the same time as GDPR, the NIS Directive goes beyond the security of private data. It focuses on availability, authenticity and integrity as well as confidentiality. The NIS Directive is in force since May 2018. Yet some EU Member States are still in the process of finalising their implementation.

Since the objective of the NIS Directive is to protect domains important to the society from cyber attacks, the sectors in scope have been chosen with care. Most of these sectors are interdependent and critical to the good function of our society: a cyber incident in one sector can trigger consequences onto other sectors.

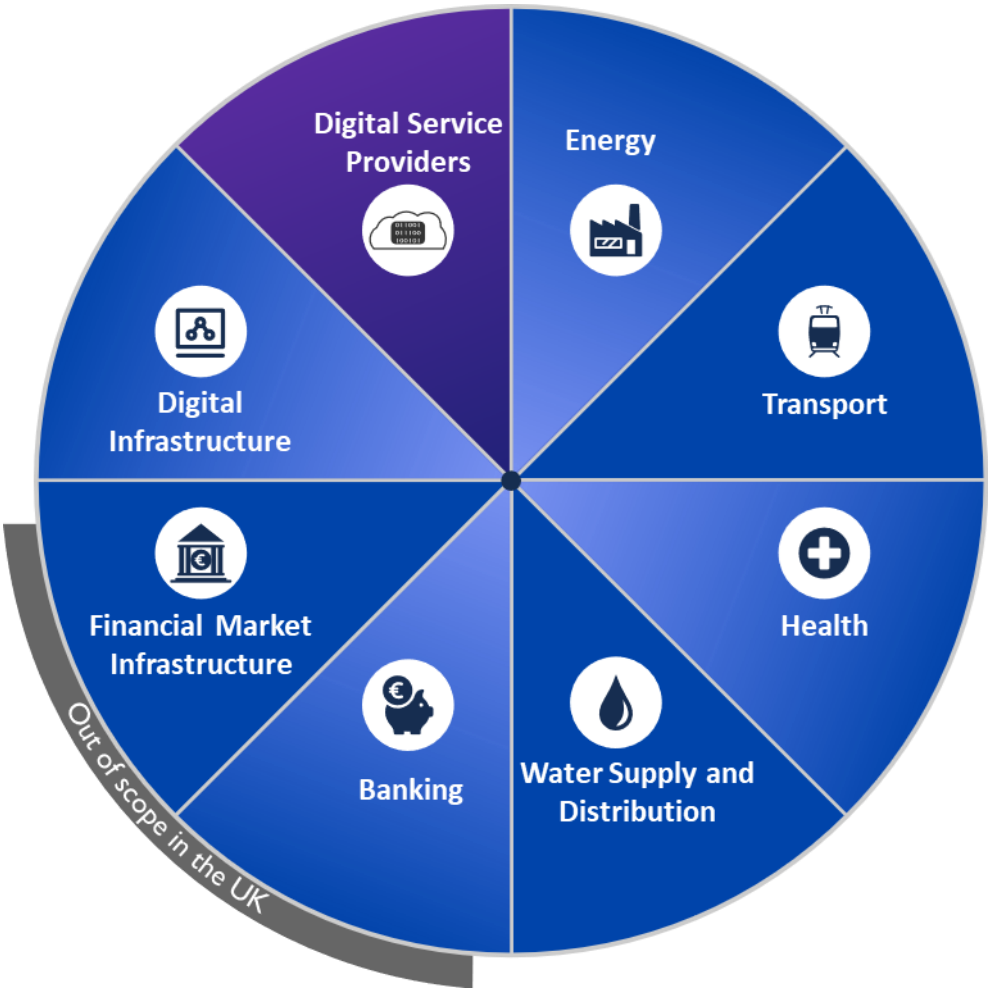


Figure 1. Sectors in Scope of the NIS Directive

The NIS Directive distinguishes two types of organisations:

- **Operators of Essential Services** (OES) that operate services that are essential for the maintenance of critical societal and economic activities. This includes operators in the sectors of energy, transport, health, drinking water supply and distribution, banking, financial market infrastructure, digital infrastructure.
- **Digital Service Providers (DSP) that are** an important resource for their users, among which we can find OESs. This includes cloud service providers, search engines, and marketplaces.

The NIS Directive also contains obligations for Member States, that must define regulatory roles (Competent Authorities), and a national CSIRT to support organisations in terms of preparedness and incident response. Member States must also contribute at EU-level via the NIS Cooperation Group and share information on a regular basis via yearly and bi-yearly reports.

For more information, please refer to the "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union".

SECURITY REQUIREMENTS IN THE NIS DIRECTIVE

The NIS Directive sets up security requirements for OESs and DSPs. While the intention is to establish a security baseline across the European Union, the NIS Directive only establishes high-level requirements. The NIS Directive does not prescribe any specific approach and Member States have adapted these requirements in their local implementation in line with their existing mechanisms, local culture, etc.

SECURITY MEASURES FOR OPERATORS OF ESSENTIAL SERVICES

The NIS Directive specifies the following:

> *"Operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed."*

The words "**appropriate and proportionate**" are the two very important keywords in the NIS Directive. It means that OES must demonstrate that their security measures are appropriate to remediate the risks they face. These security measures must also be proportionate to the risk: they are implemented promptly, without causing a damageable impact on the business, its finance, organisation, or ability to operate.

The NIS Directive requires security measures to go beyond their technical aspect, by requiring an organisational approach. This means that OES will have to identify their security objectives by taking into account people and processes on top of technologies. For instance, some OES will they need to define a governance around security, identify their critical assets, the risks they face, their staff, as well as a continuous improvement process. These requirements go way beyond IT systems: they cover OT (Operational Technologies) and any other network and information system that contributes to the essential service.

Many of times, the NIS Directive will be the occasion to formalise what is already in place. It will also be a great tool to identify gaps and priorities, refine roles and responsibilities and make sure security becomes a topic at board-level.

SECURITY MEASURES FOR DIGITAL SERVICE PROVIDERS

Similarly, DSPs must take "appropriate and proportionate" security measures to reduce the risks to their services. The NIS Directive requires that they must consider at minimum five specific domains:

"Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

(a) the security of systems and facilities;
(b) incident handling;
(c) business continuity management;
(d) monitoring, auditing and testing;
(e) compliance with international standards."

These requirements offer a way for DSPs to capitalise on their existing security investments. For example, several DSPs have already invested to comply with international standards in information security.

Incident Notification

Both OESs and DSPs must notify their competent authority and/or the national CSIRT of any incidents that could disrupt their service. They must notify these incidents without undue delay which gives OESs and DSPs the possibility to reemploy the same mechanisms as in GDPR. Note that the NIS Directive does not specify any time-bound requirement for this notification (some Member States have defined a 72 hours window after detection).

For OESs, each competent authority establishes notification thresholds that define when an incident has a **significant impact on the continuity of service**. These thresholds can depend on any of the following parameters:

- The number of users affected by the disruption of the essential service;
- The duration of the incident;
- The geographical spread with regard to the area affected by the incident.

For DSPs, they must notify incidents that have a **substantial impact on the provision of service**. The competent authority can define such incidents as a combination of:

- The number of users affected by the incident, in particular users relying on the service for the provision of their own services;
- The duration of the incident;
- The geographical spread with regard to the area affected by the incident;
- The extent of the disruption of the functioning of the service;
- The extent of the impact on economic and societal activities.

OESs and DSPs can proceed with a voluntary notification for incidents that are below these thresholds. The intent is to get a better visibility on cyber threats and enhance the security posture within a sector or even at national level.

ENFORCEMENT AND PENALTY

In the NIS Directive, the competent authority is the regulator for its sector. It can ensure compliance of its OESs/DSPs with the NIS Directive requirements and assess that their security measures are appropriate and proportionate through audits and inspections. For that purpose, OESs and DSPs need to provide evidence that they implement the requirements of the NIS Directive, and how they do it.

Contrary to other regulations, the intent of the NIS Directive is to follow a cooperative approach to enforcement. The competent authority will exchange with its OESs/DSPs to make sure they understand the requirements of the NIS Directive, assess their risks, know their gaps and establish an improvement roadmap. This stepped approach to regulation shall provide immediate benefits not only to OESs and DSPs, but to the society as a whole.

Nevertheless, competent authorities have the possibility to issue penalties. Penalties can arise in case of a breach of compliance or when the security measures (or lack of) present a risk to the essential service or the society. These penalties shall be effective, proportionate and dissuasive. Each Member State defines its own penalty regime (this could be quite high, with maximum penalties going as high as to £17M in the UK).

In the spirit of the NIS Directive, a competent authority will consider the willingness of an operator to remediate its infringement in order to reduce its penalty. For that purpose, penalties remain the last resort to enforce compliance with the NIS Directive.

WHY TAKE A LEGAL APPROACH?

The last decade has seen an increase in cyber attacks on critical infrastructure around the world with consequences on the economy and the society. It was only a matter of time before such attacks would affect European Union Member States, as the Internet has no border.

Yet, OES and DSP have shown limited investment in cyber security. This was mostly due to their limited awareness and the fact that they had confidence they were “not a target” (note that Wannacry was not a targeted attack). Yet, should an incident happen, most of these organisations tend to follow a reactive stance which could lead to undesirable effects at large scale.

The intention of the NIS Directive is to palliate this, by highlighting new compliance requirements that bring security to the board’s agenda. This is reinforced by several possible penalties that regulators can adapt to non-compliance, but also to the lack of appropriate and proportionate security measures that may cause an incident on the service.

The dissuasive penalties bring incentives to OESs and DSPs to invest in security instead of accepting the current status-quo and paying a lower fine.

CONCLUSIONS

The NIS Directive is an important new piece of regulation. Its objective is to strengthen the security of services essential to our society. It brings new obligations to Operators of Essential Services and Digital Service Providers. They must implement appropriate and proportionate security measures and notify cyber incidents without undue delay.

The NIS Directive requires a new way of thinking. A successful security approach goes beyond technical requirements. It must be endorsed at board-level whilst following a continuous improvement approach. For that purpose, every stakeholder will need to consider their current capabilities and devise improvements towards a stronger collaboration, more proactiveness, and information exchange.

In the next article, we will discuss on methods to identify the scope of the NIS Directive.

ABOUT CETOME

Dr. Cédric LÉVY-BENCHETON is the CEO and founder of Cetome. Cédric has expertise in critical infrastructure, in particular around strategic advisory and the NIS Directive. Cédric previously worked at ENISA, the European Union Cyber Security Agency. Before that, Cédric designed critical networks for public transports.

Cetome is an independent security consultancy. We work with operators of essential services, infrastructure owners and solution vendors to ensure they are ready for the NIS Directive.

We support your NIS Directive journey. We make sure that your activity is secure against cyber risks in compliance with the requirements of the NIS Directive.

Our experts have worked at ENISA, the EU Cyber Security agency, where they directly contributed to the NIS Directive and developed security measures for several sectors in scope.

We have developed our services to help implement appropriate and proportionate technical and organisational security measures as required by the NIS Directive. We follow a holistic approach that goes beyond technical and considers critical assets, third-party suppliers and the staff.

We also provide awareness and training adapted to Competent Authorities, Operators of Essential Services, Digital Service Providers and their suppliers.

Cetome
Securing a Better Future

The NIS Directive – The GDPR of Critical Infrastructure

Several recent cyber attacks have disrupted critical national infrastructure with an impact on our economy and our safety. For this reason, the European Union and its Member States (including the UK) have voted the NIS Directive to better protect our society from cyber risks.

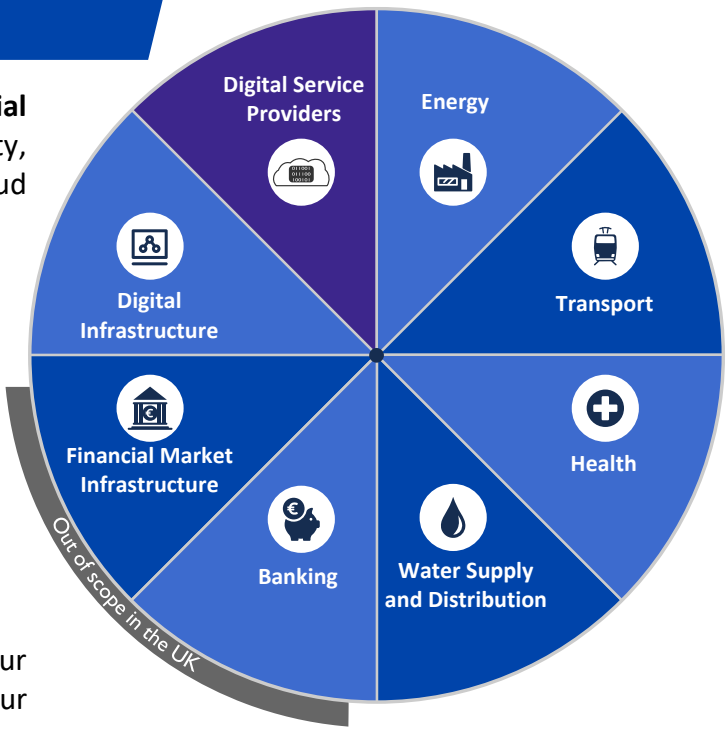
Where does it apply?

The NIS Directive applies to **Operators of Essential Services** who provide a service vital to the society, and to **Digital Service Providers** who operate Cloud services, search engines or online marketplaces.

The sectors in scope must:

- Implement appropriate and proportionate organisational and technical security measures.
- Notify significant cyber incidents to their Competent Authority without delay.

or face an important penalty!



You must comply with the NIS Directive if your organisation meets the criteria established by your Competent Authority.

Objectives of the Directive

- Understand and prevent **cyber risks** by securing network and information systems
- Augment the preparedness and **trust in critical infrastructure** across Europe and the UK
- Ensure the thorough implementation of **good security practices and cyber resilience**
- Handle incidents to **minimise impact on service** and develop lessons-learned

Compliance Timeline

NIS Directive adopted by the European Parliament
Summer 2016

May 2018
Governments published their transposition into local regulation

Governments have identified Operators of Essential Service
November 2018

Starting April 2019
Operators of Essential Services must:

- Ensure they have a security governance
- Map their gaps and risks
- Identify appropriate and proportionate security measures
- Communicate an improvement roadmap to their regulator

Operators of Essential Services must:

- Complete the deployment of appropriate and proportionate security measures
- Measure their security performance
- Demonstrate improvements in compliance

Before November 2020

Why Choose Cetome ?

Cetome
Securing a Better Future

Cetome is an **independent security consultancy**. We work with operators of essential services, infrastructure owners and solution vendors to ensure they are ready for the NIS Directive.

We support your NIS Directive journey. We make sure that your activity is secure against cyber risks in compliance with the requirements of the NIS Directive.

Our experts have worked at ENISA, the EU Cyber Security agency, where they directly contributed to the NIS Directive and developed security measures for several sectors in scope. Cetome has also trained several Competent Authorities to better understand their regulatory requirements on the NIS Directive.

Our Services

We have developed our services to help you identify and implement appropriate and proportionate technical and organisational security measures as required by the NIS Directive. We follow a holistic approach that goes beyond technical. We consider your critical assets, third-party suppliers and your staff!

We assess your existing security practice in a **readiness assessment** and identify the areas you cover and the gaps you must fill to comply with the NIS Directive.

We provide	You receive
▪ Threat and risk assessment ▪ Initial audit of your security practice ▪ Gap analysis	▶ A better vision of your security posture and priorities ▶ A support to your security strategy ▶ Mandatory compliance documents

We develop appropriate and proportionate **security requirements** based on standards and good practices to mitigate the risks on your network and information systems.

We provide	You receive
▪ Appropriate and proportionate security requirements to cover your gaps ▪ Mapping to existing standards, guidance and legal requirements	▶ Recommendations to better manage cyber risks ▶ Mandatory compliance documents

We provide **security assurance** to validate your security implementation and highlight any potential cyber risk we find.

We provide	You receive
▪ Security assurance (e.g. penetration test) ▪ Identification of residual risks	▶ Assessment of your security implementation ▶ Input for your mandatory security measurement

We recommend an **improvement programme** to complete your NIS Directive compliance and ensure you can adapt your security posture to better face new threats.

We provide	You receive
▪ Advisory on risk remediation ▪ Advisory to improve your security posture	▶ Mandatory documents for regulatory audit ▶ Input for your continuous improvement programme

Contact us

Email: info@cetome.com **Website:** cetome.com