3 The Network and Information Security (NIS) Directive. Part 2 of 2

Cyber security regulation

Continuing the previous article, in which we focused on the aspects of the Directive to be considered by online businesses, in this second article we look at how the European Union and, by extension, its Member States face a number of challenges, which are outlined below.

In 2013, the Commission put forward a proposal for a Directive on measures to ensure a high common level of network and information security across the Union. Two years later, the Parliament and Council agreed on the text of the Network and Information Security (NIS) Directive.

Main challenges posed by NIS

The European Union and therefore the Member States, after several years of debate and public consultation, face a series of challenges, which are outlined below.

It is very likely that the transposition of the NIS Directive by each Member State could lead to different cybersecurity plans with different required cybersecurity measures in the different countries of the European Union. Today, there are varying degrees of cybersecurity maturity among the Member States and, as a result, the national transposition could lead to further fragmentation of the cybersecurity plan in each country. It is probable that some countries will apply a stricter interpretation than others, as occurred with the European Data Protection Directive (95/46/EC). This diversity of interpretation could lead to an unlevel playing field in the protection of consumers and businesses, depending on the requirements applied by each Member State, and it could be a barrier to companies that wish to operate in several European countries simultaneously. It is therefore important that there be one single NIS plan to cover the entire European Union and that there is a minimum baseline of identical requirements for all countries.

The small and medium enterprises that are not required to comply with the Directive will become the weakest link in the chain. It is also expected that software and hardware manufacturers will not be affected by the Directive, which is surprising since it would seem that they should be the first to meet the basic security and privacy requirements in the design of their products and services. The fact that all these companies are not subject to compliance with minimum security measures or the reporting of incidents could potentially create a scenario in which they could become a target of cybercrime. We should not forget that small and medium companies form the biggest percentage of companies using the NIS infrastructure. The European Union should perhaps impose a minimum mandatory set of requirements and even some kind of voluntary certification that would allow for differing cybersecurity maturity levels.

Some economic challenges need to be assessed according to the degree of maturity of each Member State, as there are already some countries with cybersecurity plans and even various national CSIRTs. It will also be important for ENISA to be provided with sufficient funds to coordinate the various national CSIRTs.

It is not currently known what the specific powers of a National Competent Authority (NCA) and National Computer Security Incident Response Team (CSIRT) will be. There is also no guidance on the overlapping reporting obligations under the various regulations, such as NIS and the future General Data Protection Regulation (GDPR). Similarly, no account has been taken of the possibility that some critical operators could be subject to simultaneous notification to various national and international regulators. For example, in the case of a Spanish bank, a personal data breach in a significant cyber incident must be simultaneously notified to the national data protection regulator, the competent critical infrastructure regulatory authority, the Ministry of the Interior and the European Central Bank. These challenges highlight the large number of

regulators that can be demanding the same responsibilities, creating regulatory duplication and, therefore, adding more complexity and costs for businesses and governments. A single notification mechanism in the style of a "one-stop-shop" could improve the effectiveness of notifications and reduce costs and complexity.

It is also a challenge to identify the most effective way to report incidents between entities and the standards to use, as well as to establish the same requirements in all Member States, thereby avoiding different implementations and obtaining a more effective sharing of incidents with public and private entities. It would also be desirable to contemplate a legal way to share incidents involving personal data, such as, for example, the IP addresses of malware-infected computers involved in phishing campaigns targeting public or private entities. In this way, the entities could be more proactive and obtain a significant reduction in cyber-attacks through effective collaboration between public and private companies.

Although the technical and organizational measures imposed on the companies affected by the NIS Directive initially do not require a product or service to be designed, developed or manufactured in any particular way, some countries might be tempted to impose a registration, approval or certification process for products and services. If the objective of such a provision was to foster a minimum degree of maturity in businesses, it would be essential for all Member States to reach an agreement, so as to prevent fragmentation. Possibly, a good choice would be to create voluntary but incentivised certification with varying levels of maturity, based on internationally recognized standards, such as the European Telecommunications Standards Institute (ETSI) or the IEEE-SA standards.

Conclusion

If necessary, the authorities with the power to transpose the NIS Directive could investigate and sanction cases of non-compliance. They must therefore have the power to make assessments of the level of cybersecurity and the measures required of company information systems. They could also require cybersecurity audits to be performed by third parties. In the absence of more information, there are concerns about what the requirements will be regarding minimum safety measures, whether they will be based on internationally recognized standards or audits, such as ISO 27001, NIST or SSAE16, or whether new standards will be created. It is also not known whether these standards and audits will be common throughout the European Union or if each country will adopt its own, leading to further fragmentation.

While the NIS Directive is certainly a major step forward in improving cybersecurity in Europe, we will have to wait and evaluate how the European Commission and ENISA will solve these challenges by enacting laws and guidelines, which are expected to provide greater detail regarding the implementation of strategic cooperation plans or the specifications and standards that may be used for NIS.

It is expected that in the coming months the Parliament and the Council of the European Union will formally approve the Directive, after which it will be published in the Official Journal of the European Union. Member States will have twenty-one months to transpose the NIS Directive into national law and an additional six months to identify the essential service operators.

DISCLAIMER

This document has been prepared by BBVA Research Department, it is provided for information purposes only and expresses data, opinions or estimations regarding the date of issue of the report, prepared by BBVA or obtained from or based on sources we consider to be reliable, and have not been independently verified by BBVA. Therefore, BBVA offers no warranty, either express or implicit, regarding its accuracy, integrity or correctness.

Estimations this document may contain have been undertaken according to generally accepted methodologies and should be considered as forecasts or projections. Results obtained in the past, either positive or negative, are no guarantee of future performance.

This document and its contents are subject to changes without prior notice depending on variables such as the economic context or market fluctuations. BBVA is not responsible for updating these contents or for giving notice of such changes.

BBVA accepts no liability for any loss, direct or indirect, that may result from the use of this document or its contents.

This document and its contents do not constitute an offer, invitation or solicitation to purchase, divest or enter into any interest in financial assets or instruments. Neither shall this document nor its contents form the basis of any contract, commitment or decision of any kind.

In regard to investment in financial assets related to economic variables this document may cover, readers should be aware that under no circumstances should they base their investment decisions in the information contained in this document. Those persons or entities offering investment products to these potential investors are legally required to provide the information needed for them to take an appropriate investment decision.

This report has been produced by the Digital Regulation Unit:

Chief Economist for Digital Regulation Unit
Álvaro Martín
alvaro.martin@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Israel Hernanz
israel.hernanz@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

With the contribution of:

Francisco Borja Larrumbide Martínes
fborja.larrumbide@bbva.com

Alfonso Arellano
alfonso.arellano.espinar@bbva.com

BBVA Research

Group Chief Economist
Jorge Sicilia Serrano

Developed Economies Area
Rafael Doménech
r.domenech@bbva.com

Spain
Miguel Cardoso
miguel.cardoso@bbva.com

Europe
Miguel Jiménez
mjimenezg@bbva.com

US
Nathaniel Karp
Nathaniel.Karp@bbva.com

Emerging Markets Area

Cross-Country Emerging Markets Analysis
Alvaro Ortiz
alvaro.ortiz@bbva.com

Asia
Le Xia
le.xia@bbva.com

Mexico
Carlos Serrano
carlos.serranoh@bbva.com

Turkey
Alvaro Ortiz
alvaro.ortiz@bbva.com

LATAM Coordination
Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Peru
Hugo Perea
hperea@bbva.com

Venezuela
Julio Pineda
juliocesar.pineda@bbva.com

Financial Systems and Regulation Area
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Financial Systems
Ana Rubio
arubiog@bbva.com

Financial Inclusion
David Tuesta
david.tuesta@bbva.com

Regulation and Public Policy
María Abascal
maria.abascal@bbva.com

Digital Regulation
Álvaro Martín
alvaro.martin@bbva.com

Global Areas

Economic Scenarios
Julián Cubero
juan.cubero@bbva.com

Financial Scenarios
Sonsoles Castillo
s.castillo@bbva.com

Innovation & Processes
Oscar de las Peñas
oscar.delaspenas@bbva.com

Contact details:

Azul Street, 4
La Vela Building - 4 and 5 floor
28050 Madrid (Spain)
Tel.: +34 91 374 60 00 and +34 91 537 70 00
Fax: +34 91 374 30 25
bbvaresearch@bbva.com
www.bbvaresearch.com