

# White Paper

**HardenStance**

## Telco Security Takeaways from the NIS2 Directive

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by



November 2023



**HardenStance**

*"Trusted Research, Analysis and Insight in IT  
& Telecom Security"*

## Executive Summary

- The NIS2 Directive greatly expands the power of regulators to direct how EU-based telcos and other Essential or Important Entities operationalize cybersecurity.
- For the first time, NIS2 mandates cyber risk management principles; stiffer penalties and greater management accountability for cybersecurity breaches; and sets high expectations for reporting cybersecurity incidents to regulators.
- Effective enforcement will be key. There is a risk of counter-productive or even risk-inducing outcomes if provisions relating to vulnerability disclosure, threat intelligence sharing, and incident reporting are not implemented with due care.

## Telecoms is just one sector addressed by NIS2

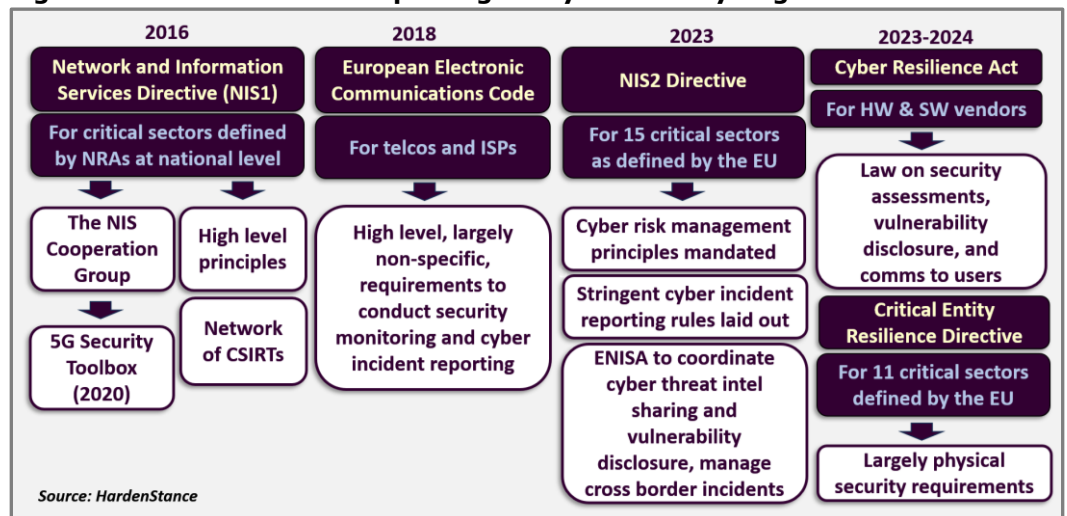
EU-based telcos are used to complying with cybersecurity regulations enforced by their National Regulatory Authorities (NRAs). In recent years, the greatest impacts have been felt from national implementations of the European Electronics Communications Code (EECC) of 2018 and the 5G Security Toolbox of guidelines that was brought into effect by the first Network and Information Services (NIS) Directive of 2016 (see **Figure 1**).

The second NIS Directive, NIS2, came into effect in January 2023. It substantially raises the bar in terms of what is expected for how telcos and other critical sectors of industry frame and execute on their cybersecurity operations. Telcos – or “providers of public electronic communications networks” as the Directive calls them – are classified as “Digital Infrastructure.” This is one of the eight categories of “Essential Entity” the Directive addresses. Whereas Essential Entities are held to the highest cybersecurity standards in NIS2, a further seven categories of “Important Entity” are subject to less stringent requirements. For example, they should only be subjected to what Article 122 refers to as “a light, ex post only, supervisory regime”, whereas Essential Entities should face “a comprehensive ex ante and ex post supervisory regime.” Article 2 Paragraph 2 specifies that NIS2 applies to all telcos “regardless of their size.”

The NIS2 Directive is the centrepiece of EU cybersecurity law. Member states have until October 2024 to apply it in national law. As shown in **Figure 1**, the Cyber Resilience Act (CRA) will certainly impact telcos but is primarily aimed at driving up standards of cybersecurity hygiene practised by hardware and software vendors whose products may connect to telco networks (including networking products). The Critical Entity Resilience (CER) Directive affects telcos too, albeit mainly as regards physical security operations. It also addresses satellite communications (which the NIS2 Directive doesn't).

*NIS2 substantially raises the bar in terms of what is expected of how telcos and other critical sectors of industry frame and execute on their cybersecurity operations,*

**Figure 1: Telecom Sector-Impacting EU Cybersecurity Regulations 2016 - 2024**



**Figure 2: The NIS2 Directive and the European Electronic Communications Code (EECC) Compared**

Requirement	NIS2 Directive (2023)	European Electronic Communications Code (2018)
Adoption of cyber risk management principles	Mandated	Not mentioned
Management's obligations	"Approve and oversee implementation."	Not mentioned
Timeframe in which a significant incident to be initially reported	Within 24 hours	"Without undue delay"
Cyber threat intelligence sharing	Mandated across stakeholders.	Not mentioned
Penalties for non-compliance	Up to 2% of annual turnover	"Appropriate, effective, proportionate and dissuasive."
Management of cross border cybersecurity incidents	Assigned to EU CyCLONe	Not mentioned

Source: HardenStance

*This White Paper addresses that subset of features of the NIS2 Directive that herald substantial change in how cybersecurity has to be done by telcos in the EU.*

This White Paper has a very narrow objective:

- It doesn't address all the key obligations mandated by the NIS2 Directive. These will be brand new requirements for some Entities which the EU is addressing with cybersecurity rules for the very first time with NIS2. In the case of telecoms, however, several NIS2 requirements are already partially or largely practised. This may be due either to previous national or EU legislation, or because the telecom sector already adheres to aspects of NIS2, independent of any regulatory mandate.
- This paper doesn't address all the cybersecurity mandates arising from all relevant EU legislation up to and including the NIS2 Directive. This would require a much longer page-count. Hence it doesn't address pre-existing regulations and their impacts such as the EECC or 5G Security Toolbox of 5G security recommendations.

Instead, this White Paper addresses that subset of features of the NIS2 Directive that herald substantial change in how cybersecurity has to be done by telcos in the EU.

## What's new in NIS2 from a telco point of view?

As shown in **Figure 2**, NIS2 imposes much more stringent obligations on telcos than the 2018 EECC. The seven key aspects of NIS2 that mandate new approaches to how telecom operators must frame and operationalize cybersecurity are highlighted below:

- 1 Management obligations are established in law.
- 2 A cyber risk management approach is mandatory.
- 3 Better vulnerability disclosure and threat intelligence sharing are encouraged.
- 4 There are stringent new timescales for submitting cyber incident reports.
- 5 EU CyCLONe is established for managing EU-wide cybersecurity incidents.
- 6 Substantial fines are payable for non-compliance.
- 7 The regulatory playing field with the webscalers is levelled up.

Each of these seven aspects is now discussed in detail, together with commentary and guidance on the opportunities and challenges they each present.

## 1. The obligations of management are established in law

NIS2 establishes that the management team of a telco is directly responsible for cybersecurity in law. Chapter IV, Article 20, Paragraph 1 states:

*"Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities, oversee its implementation and can be held liable for infringements."*

This is an important step and a good thing. In member states today, national laws tend not to be so explicit about telco management's responsibility for approving and overseeing cybersecurity strategy. The resulting ambiguity can leave management free to offload responsibility onto the CISO and their team in the event of a major breach. NIS2 eliminates this ambiguity. It holds management's feet to the fire in law – often for the first time. One high profile law firm, Sidley Austin LLC, interprets the Directive as meaning that "senior management individuals could face administrative fines and/or a potential ban/discharge from managerial functions." (See 'More Information' at the end of this paper.) Even if this scenario isn't likely, the theoretical threat of it still has potential to influence management behaviours.

*NIS2 eliminates ambiguity. It holds management's feet to the fire in law – in many cases for the first time.*

## 2. A cybersecurity risk management approach is mandatory

The term "cyber risk management" appears 53 times in the Directive. Article 22 states:

*"This Directive sets out the baseline for cybersecurity risk-management measures and reporting obligations across the sectors that fall within its scope."*

A risk management approach is a key enabler of a mature cybersecurity posture. Legacy compliance-based approaches do no more than implement largely technological or operational standards mandated by the regulator. A risk management approach is driven by continuous assessments of the risks to the business as a whole - and mapping investment to the highest risks. This involves quantifying risk. At a high level, a potential cybersecurity incident that is assessed as having an estimated cost of \$100 million, with a 40% chance of happening in any one year, is considered a \$40 million-a-year risk.

With a risk management approach, the risk of penalties arising from non-compliance with regulations becomes just one of many risks to manage. Cyber risk management shouldn't be an isolated discipline; it should form part of a broader risk management strategy for managing legal, commercial and other types of business risk. Consistent with that, the NIS2 Directive mandates in Article 21 Paragraph 2, that:

*"The cyber risk management measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents."*

As shown in **Figure 3**, the Directive lays out a baseline of measures that are considered necessary for cyber risk management. These are basic staples of mature cybersecurity

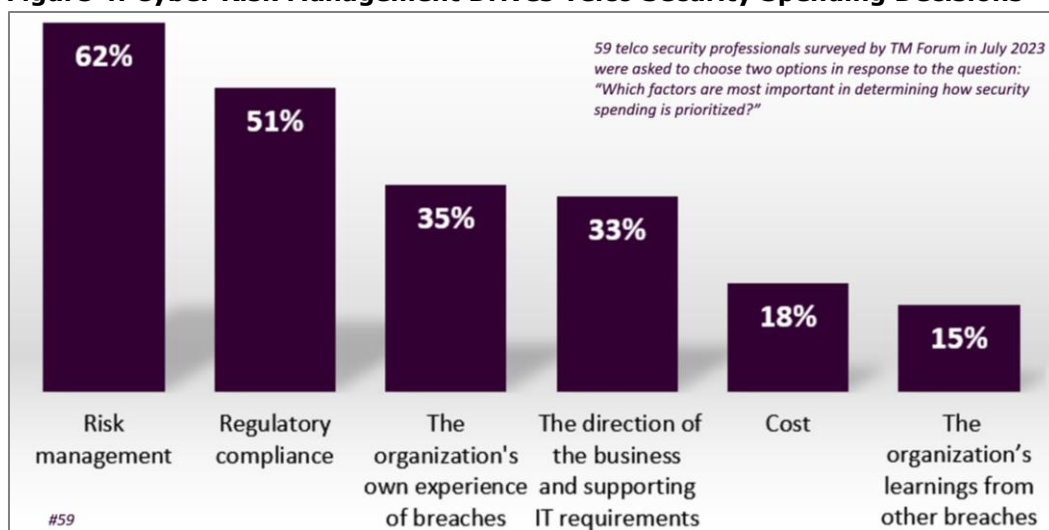
**Figure 3: Minimum Cyber Risk Management Measures as Mandated by NIS2**

Policies on risk analysis and information system security	Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
Human resources security, access control policies and asset management	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
Use of multifactor authentication (MFA) or continuous authentication solutions, secured voice, video and text communication and secured emergency communication systems within the entity, where appropriate	Policies and procedures to assess the effectiveness of cyber risk management measures
Basic cyber hygiene practices & training	Business continuity (backup management, disaster recovery, crisis management)
Supply chain security	Incident handling

Source: The NIS2 Directive/HardenStance

Potentially, among the most significant changes introduced is the new role it creates for government to encourage and orchestrate better vulnerability disclosure and threat intel sharing.

**Figure 4: Cyber Risk Management Drives Telco Security Spending Decisions**



Source: TM Forum's "Cybersecurity Strategies: Risk Management Moves into the Telco Spotlight"

practice. Today, however, the quality and consistency of implementation varies a lot between different European telcos, and even across different parts of the same telco. **Figure 4** provides evidence that telcos have already started aligning with the NIS2 Directive on this ahead of the implementation deadline. Taken from a July 2023 TM Forum survey of telco security professionals – world-wide rather than just in Europe – it shows that cyber risk management is considered more important than simple or traditional regulatory compliance in determining how security spending is prioritized.

### 3. Better vulnerability disclosure and threat intel sharing

Potentially, among the most significant changes NIS2 introduces is the new role for government to encourage and orchestrate better vulnerability disclosure and cyber threat intelligence sharing. **Figure 4** demonstrates just one aspect of the need for this to improve in telecoms. As shown, telecom security professionals said that learnings from other organizations' breaches are currently much less important for prioritizing cybersecurity spending than learnings from their own organization's direct experience.

The Directive establishes a legal framework for better risk and threat information sharing between member states; between the private and public sectors; as well as between different sectors of critical infrastructure. This certainly promises, or aims for, a major break with precedent. Today, cybersecurity researchers, analysts and threat intelligence specialists leverage informal networks of trusted personal relationships, as well as international standards with privacy or security safeguards built in. They use these to navigate their way around data privacy regulations as well as legal constraints on their work imposed by local, national and international law and law enforcement. NIS2 brings specific and direct regulatory oversight to aspects of these activities for the first time.

The Directive treats vulnerability disclosure and threat intelligence sharing separately. In the case of vulnerability disclosure, Article 62 states:

*"ENISA should establish a European vulnerability database where entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, as well as the competent authorities and the CSIRTs, can disclose and register, on a voluntary basis, publicly known vulnerabilities for the purpose of allowing users to take appropriate mitigating measures."*

The EU's vulnerability disclosure regime is established across both NIS2 and drafts of the new Cyber Resilience Act. Most of the detail – including the controversial proposal for software publishers to disclose unpatched vulnerabilities to government agencies within 24 hours of exploitation – is in the Cyber Resilience Act. However, in the first

---

instance it is the NIS2 Directive that empowers ENISA to create and manage a huge, centralized database of vulnerabilities. That's a database that dozens of government agencies can potentially have authorized, real-time, access to - and hackers could potentially gain unauthorized access to as well. There is potential risk here that needs to be thought through and mitigated.

Reflecting the telecom sector's relative maturity compared with some other sectors of critical industry, the GSMA and ETSI already have Common Vulnerability Disclosure (CVD) programs in place. Telco security professionals should therefore expect to be called upon by their NRAs, and potentially by ENISA, to play a prominent role in picking a careful path to executing on the EU's vision in this area.

Whereas the Cyber Resilience Act contains the bulk of detail relating to vulnerability disclosure, the framework for threat intelligence sharing is almost entirely front-loaded in the NIS2 Directive. Article 119 explicitly recognizes some complicating factors:

*Appropriately, the Directive's emphasis is less on mandating how it is to be achieved and more on empowering regulators to "enable" better sharing on a "voluntary" basis.*

*"In the absence of guidance at Union level, various factors seem to have inhibited such intelligence sharing, in particular uncertainty over the compatibility with competition and liability rules."*

For the most part, NIS2 sketches out a high level framework. It leaves regulators and stakeholders to exercise their judgement as to how they should inch towards achieving better outcomes. Appropriately, the Directive's emphasis is less on mandating how it is to be achieved and more on empowering regulators to "enable" better sharing on a "voluntary" basis. There are, nevertheless, some mandates in this area. The most notable of these are in Article 7 and Article 120 cited below:

*"Member States shall in particular adopt policies including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing."*

*"It is thus necessary to enable the emergence at Union level of voluntary cybersecurity information-sharing arrangements."*

Article 103 (applicable to all Entities) and Article 104 (applicable only to telcos and ISPs) also mandate the following:

*"Where applicable, essential and important entities should communicate, without undue delay, to their service recipients any measures or remedies that they can take to mitigate the resulting risks from a significant cyber threat.....The provision of such information about significant cyber threats...should be free of charge and drafted in easily comprehensible language."*

*"Providers of public electronic communications networks should....inform their service recipients of significant cyber threats and of measures they can take to protect the security of their devices and communications."*

Whether it's mandated by national regulations or practised independently of them, sharing some threat intel with customers is already common practice for a lot of telcos. A legal requirement to make this "free of charge" and "easily comprehensible" may not be so familiar, although the term "where applicable" appears to create wiggle room.

The net impact of NIS2 on vulnerability disclosure and threat intelligence sharing in the EU is likely to be substantial, although there could potentially be as much risk on the downside as opportunity on the upside. Company lawyers and risk management professionals will be incentivized to scrutinize the day-to-day operating practices of some of their cybersecurity professionals more closely than in the past. This could have a chilling effect on collaboration – quite the opposite of what the Directive intends. The challenge in this area will be for leaders to step up to develop and share operational best practices that can mitigate risk as a condition of making progress.

#### 4. Stringent timescales for submitting cyber incident reports

Today, cybersecurity best practice is predicated on the assumption that a subset of cyber attacks will be at least partially successful. Incidents will happen. Consistent with the principle of cyber resilience, detecting, mitigating and recovering from successful intrusions quickly and effectively is as important as blocking the large majority of intrusion attempts altogether.

Defining an appropriate timeframe for making regulated companies report significant cybersecurity incidents is a highly complex challenge. There are bad, unacceptable reasons why an organization might want to delay reporting or share very little information. For example, it may lack information due to a weak cybersecurity posture or it may put its own interests above those of its customers and other stakeholders.

##### There are some good reasons for delaying reporting

There are also some entirely acceptable reasons for delay. In the first couple of days following an incident it can be genuinely difficult, if not impossible, to accurately assess what has occurred and what the impact is. Initial assumptions often prove to be incomplete or plain wrong. Inaccurate reports run the risk of either triggering a false alarm or fostering complacency. With some severe incidents, it can be very challenging to get to the bottom of exactly how many customers or supply chain partners are impacted, and how badly, within weeks (or even months).

Importantly, NIS2 does explicitly recognize the complexity of the challenge in incident reporting. It also implicitly recognizes the need for flexibility in the enforcement of the rules. Specifically, Article 102 states:

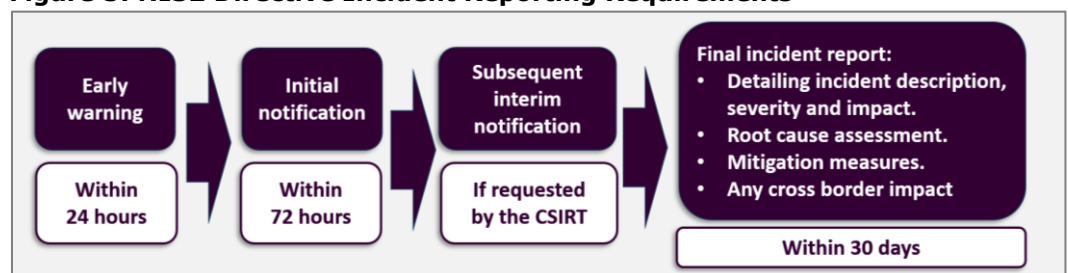
*"Member States should ensure that the obligation to submit that early warning, or the subsequent incident notification, does not divert the notifying entity's resources from activities related to incident handling that should be prioritised, in order to prevent incident reporting obligations from either diverting resources from significant incident response handling or otherwise compromising the entity's efforts in that respect."*

Article 23, Paragraph 3 specifies that an incident shall be considered to be significant if:

- (a) *it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;*
- (b) *it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.*

However, the Directive does not go on to define "severe" operational disruption or financial loss or "considerable" damage. It leaves these critical definitions to individual NRAs. However NRAs choose to define them, the Directive is nevertheless very stringent when it comes to specifying the timeframe within which incidents must be reported. As shown in **Figure 5**, early warning, initial and final incident reports must be submitted within 24 hours, 72 hours and 30 days, respectively.

**Figure 5: NIS2 Directive Incident Reporting Requirements**



Source: The NIS2 Directive/HardenStance

*Defining an appropriate timeframe for making regulated companies report significant cybersecurity incidents is a highly complex challenge.*

## Threat Detection and Response is Inadequate in Telecom Networks

A telco's visibility, threat monitoring, detection and response capabilities in its internal enterprise IT environment tends to be relatively good. Employees have a legitimate need for direct access to internal operational systems and sensitive corporate data. That means misbehaviour by employees – whether benign or malicious – is a relatively high risk to the telco organization. Hence, telcos tend to invest in it.

By contrast, in the case of a telco's public network infrastructure, where the risk to the telco organization itself is less, threat visibility, monitoring, detection and response tend to be far less developed. For example, most mobile operators, including operators in the EU, tend to have little or no capability to detect and mitigate cyber threats in the Radio Access Networks (RAN).

An implicit goal of the NIS2 Directive is to correct this present day imbalance. This is an area that operators are going to have to invest more in to be able to meet NIS2's new incident reporting requirements. Better threat intelligence sharing comes into this too, since the all-important sharing of contextual threat intelligence is key to driving faster detection and better response outcomes.

For telcos and other regulated businesses operating in some EU member states, such as the Netherlands, an initial early warning report within 24 hours is already a requirement. In many member states, however, current national laws require initial reports according to the much looser "without undue delay" type of requirement specified by the EEC.

Similarly, there may already be some member states that already require that their telcos submit a final incident report within 30 days. However, it's a safe assumption that not many member states already require all their telcos to comply with all of NIS2's 24 hour, 72 hour and 30 day deadlines. For many, probably most, of Europe's telcos, at least one or two of the NIS2 reporting timelines will be new and more demanding than what is expected of them today. For some, all three will be.

The goal with the incident reporting targets therefore seems to be pretty clear. It is a regulatory regime for cybersecurity that demands that telcos report incidents faster and in more detail than many of them currently do. But it is also a regime where enforcement discriminates accurately and intelligently between legitimate and illegitimate reasons for failing to comply to the exact letter of the law each and every time a report has to be filed. The quid pro quo has to be that telcos must engage with NRAs constructively – and be seen to engage constructively. It's in their interests to do so.

## 5. EU CyCLONe is established for managing EU-wide incidents

The European Cyber Crisis Liaison Organisation Network (EU CyCLONe) is a cooperation network for Member State national authorities in charge of cyber crisis management. The network was launched in 2020 and is formalized with NIS2. As stated in Article 16:

*"EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies."*

ENISA provides the CyCLONe Secretariat, infrastructures and tools to enable effective cooperation to respond to large-scale and cross-border cyber incidents. ENISA also supports the organisation of exercises for CyCLONe members. Member states, and major national telcos already collaborate with one another on cross-border incident management as well as with peers throughout the world. A pan-European agency for coordinating the management of large-scale cyber incidents has potential to lead to better outcomes but it's very early days for gauging what it will look like and how it will function operationally. It will likely take a number of years for

*In many member states, current national laws require initial reports according to the much looser "without undue delay" type of requirement specified by the EEC.*

CyCLONE to displace or supercede current, informal arrangements and reach the full potential envisaged for it by NIS2. The political, legal and operational aspects of member states delegating some part of what clearly forms part of national security operations to a supra-national European agency will be challenging. Before that even comes to be grappled with, nation states will need to implement NIS2 in national law.

## 6. Substantial fines are payable for non-compliance

Article 34, Paragraph 4 states:

*"Member States shall ensure that where they infringe Article 21 or 23, essential entities are subject to administrative fines of a maximum of at least €10,000,000 or of a maximum of at least 2% of the total worldwide annual turnover, whichever is higher."*

Set against the context of the NIS1 Directive and the EECC, a fine of 2% of turnover is quite an escalation in risk exposure for a telco. NIS1 did not specify any penalties at all. As shown in **Figure 2**, the EECC prescribes only that fines should be "appropriate, effective, proportionate and dissuasive." The risk of higher regulatory fines is already priced in in the case of General Data Protection regulation (GDPR). This allows for fines of up to 4% of annual turnover, although many of the measures needed to align with NIS2 are new and distinct from those required for GDPR compliance.

The UK - where the new Telecommunications Security Act allows fines of up to 10% of turnover for non-compliance - is a relevant comparison for telcos and other Essential Entities covered by NIS2. Another comparison is the lower 1.4% ceiling that NIS2 establishes for Important Entities.

## 7. The playing field with the webscalers is levelled up

In terms of how regulation intersects with business goals, one of the things telecom operators care most about is levelling the regulatory playing field with the world's big web-scalers - Apple, AWS, Facebook, Google, Microsoft et al.

Europe's telcos know little else besides a world of being regulated entities operating under government license - including in the cybersecurity space. How telcos conduct their security operations was regulated at some level by their NRAs decades before the EU started exerting its authority.

Until now, it has been different for webscalers. They are, of course, covered by the EU's GDPR. Indeed Amazon, Facebook and Google have received some of the largest fines for GDPR violations. However, GDPR rules relate to privacy rather than cybersecurity. And until now, webscalers have managed to remain largely untouched by the EU's extension of its authority into the cybersecurity domain.

The NIS2 Directive changes this. As shown in **Figure 6**, Annex 1 specifically states that "cloud computing service providers" are included in the Digital Infrastructure category of Essential Entities alongside telecom operators. Hence, AWS, Azure and Google Cloud Platform (GCP) must comply.

**Figure 6: Cloud Providers are Classified as "Digital Infrastructure Entities"**



Source: Definition of 'Digital Infrastructure Entities', Annex 1, The NIS2 Directive

*Set against the context of the NIS1 Directive and the EECC, a fine of 2% of turnover is quite an escalation in risk exposure for a telco.*

*New vulnerability disclosure and threat intelligence sharing regimes may take a while to come into effect, though. In many cases they probably should.*

Annex 2 also cites providers of “online marketplaces”, “online search engines” and “social networking services platforms” among the seven types of Important Entities covered. Clearly, the EU expects Apple, Facebook and Google to comply. They can be expected try every legal trick in the book to find ways of exempting themselves. They may even be tempted to risk non-compliance and just suck up whatever fines come their way, as they have tended to with GDPR. That said, the general political mood – not just in the EU but throughout the world – does nevertheless seem to be shifting in favour of holding the webscalers feet closer to the fire from a general regulatory standpoint.

## Timing of impacts and the future EU legislation

Different aspects of the NIS2 Directive will start impacting the cybersecurity strategy and operations of EU-based telcos at different times. National implementations of NIS2 may happen over a more concentrated period than in the case of the EECB but it’s worth noting that whereas Estonia implemented the latter in 2018, Ireland didn’t get it done until earlier this year.

The direction of NIS2 was clear for a long time before it came into effect this year. The deadline for adoption in national law is still a year away. For the most part, NRAs should have no time for any kind of grace period once the Directive is adopted in national law. New vulnerability disclosure and threat intelligence sharing regimes may take a while to come into effect, though. In many cases that will be appropriate in order to assure the right scope for achieving material improvements. As discussed, it will likely take years for EU CyCLONE to wield its authority to good effect.

The historical pattern of EU legislation suggests that what is left to member states to determine at the national level in one piece of legislation, tends to get harmonized at EU level the next time round. For example, NIS2 harmonizes the classification of Essential and Important Entities where NIS1 left the classification up to member states. Assuming the same continuum, it’s easy to see how a future NIS3 or equivalent Directive could go about harmonizing things like the definition of a significant incident. It could include more granular legal mandates with respect to how threat intelligence is shared or how responsibilities should be shared between member states and EU CyCLONE. ■

## More Information

- [Watch HardenStance’s November 8th 2023 webinar “Aligning with the NIS2 Directive” featuring Nokia and Cyber Threat Alliance.](#)
- [TM Forum's "Cybersecurity Strategies: Risk Management Moves Firmly into the Telco Spotlight" \(September 2023\)](#)
- [HardenStance Briefing: "Threat Intel in Telecoms - TTIS 2023" \(August 2023\)](#)
- [HardenStance webinar: "The End of Laissez Faire in Telecom Cybersecurity Regulation" featuring Ofcom, the NCSC and Nokia \(April 2023\)](#)
- [Nokia White Paper: "Demystifying the NIS2 Directive" \(2023\)](#)
- [About EU CyCLONE](#)
- ["Sidley Austin LLC Jan 2023: "Senior Management Could Face Fines or Discharge."](#)
- [Register for HardenStance’s “Telecom Threat Intelligence Summit” \(June 2024\)](#)

## About Nokia

At Nokia, we create technology that helps the world act together. As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry. Through networks that sense, think and act, we work with our customers and partners to create the digital services and applications of the future. See [here](#).

---

## About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, MEF, The GSMA and ETSI. HardenStance is also a recognized Cyber Threat Alliance 'Champion'. To learn more visit [www.hardenstance.com](http://www.hardenstance.com)

## HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.