Cybersecurity Update: NIS2

Authors:
Ian Duffy, Partner, Arthur Cox LLP and Member of Compliance Institute's Data Protection & Information Security (DP&IS) Working Group

Ciara Anderson, Senior Associate, Technology, Arthur Cox LLP.

Vivian Spies, Associate, Technology & Innovation Group, Arthur Cox LLP.

The Network and Information Systems Directive (EU) 2022/2555 or "NIS2" aims to modernise the legal framework surrounding cybersecurity across the EU to account for a rapidly growing technological and digital environment. NIS2 replaces its predecessor NIS1 which applied from 2018, whilst broadening its scope and providing more comprehensive and prescriptive cybersecurity risk management and reporting measures.

Ireland missed the transposition deadline of 17 October 2024. As at the date of this article, the General Scheme for the National Cyber Security Bill 2024 has been published however the legislative process has not yet progressed further.

Scope

Organisations not previously captured by NIS1 may find themselves subject to NIS2. NIS2's expanded scope covers sectors such as B2B managed service providers, manufacturing, and research. Therefore, it is important that organisations familiarise themselves with the scope of NIS2. NIS2 also expands certain sectors previously captured by NIS1. For example, NIS2 broadens the scope of the digital infrastructure sector to capture cloud computing service providers, data centre service providers and providers of public electronic communications networks and services.

Importantly, the Digital Operational Resilience Act or "DORA" is considered *lex specialis* to NIS 2 and covers much of the same substance. This means that financial entities subject to DORA do not also have to comply with NIS2.

Essential and important entities

NIS1 was split between obligations applicable to "operators of essential services" and "digital service providers". Under NIS2, in-scope entities are instead classified as "essential" or "important" depending on their sector and size. The national competent authority (which will depend on the sector) may also designate an entity as "essential" if, for example, the entity is the sole provider of the service in Ireland and such service is considered critical.

Cybersecurity risk management measures

NIS2 is more prescriptive than NIS1 in respect of cybersecurity risk management measures. NIS2 requires entities to take appropriate and proportionate technical, operational and organisational measures to manage the risks to their systems and prevent or minimise the impact of cyber incidents in the provision of their services. For example, NIS2 requires in-scope entities to undertake due diligence on their supply chain cybersecurity and provide appropriate cybersecurity training to staff. Additionally, entities are encouraged to include cybersecurity risk management provisions in their contracts with suppliers.

Incident reporting

NIS2 requires entities to report "significant" cybersecurity incidents to the computer security incident response team or "CSIRT" which in Ireland is the National Cyber Security Centre.

In the event of a significant cybersecurity incident, entities are required to follow a four-step incident reporting process. Entities must submit to the CSIRT:

1. An initial notification within **24 hours** of becoming aware of the significant incident
2. An initial risk assessment and any additional information not provided in the initial notification **within 72 hours** of awareness
3. An intermediate status report if requested to do so
4. A final report within **one month** of the initial risk assessment

If the entity believes that the cybersecurity incident may have adversely affected the provision of its services, it must also notify its customers.

Enforcement

Important entities may be subject to administrative fines of up to €7 million or 1.4% of their global annual turnover. Essential entities are subject to greater supervision and enforcement measures such as ad hoc audits and greater administrative fines of up to €10 million or 2% of their global annual turnover.

NIS2 holds the management bodies of in-scope entities ultimately responsible for overseeing the implementation of cybersecurity risk management measures and these individuals may be held personally liable for non-compliance. Further, if an essential entity is found to be non-compliant with NIS2 and action is not taken to remedy deficiencies, the entity may have its authorisation temporarily suspended or individuals at management level may be temporarily suspended from discharging managerial responsibilities.

Link to NIS2 Video Series by **Vivian Spies, Foreign registered lawyer, Technology and Innovation Group, Arthur Cox** Network and Information Security Directive (NIS2) - Arthur Cox LLP