The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 15 June 6, 2018

NISD

Beyond GDPR: The E.U.'s Expanding Cybersecurity Regime

By Megan L. Brown, Matthew J. Gardner, Michael L. Diakiwski, Wiley Rein

As companies implement data privacy and security policies to comply with the General Data Protection Regulation (GDPR), other European cybersecurity directives have garnered less attention. While the May 25, 2018 enforcement date for the GDPR loomed large, the Directive on the security of networks and information systems (known as the NIS Directive) also had a key deadline in May and warrants careful attention by certain business sectors. In addition, there are other European efforts aimed at establishing security and certification standards for internet-connected devices. United States interests should prepare for all of these initiatives.

See also "Direct From the Irish Data Commissioner: GDPR Enforcement Priorities (Part Two of Two)" (May 2, 2018).

Overview of the NIS Directive

Adopted by the European Parliament on July 6, 2016, the NIS Directive entered into force in August 2016. E.U. Member States had 21 months to integrate its requirements into their own national laws and an additional six months to identify the companies which are subject to NIS Directive compliance. The Directive is part of the European Commission's (EC's) cybersecurity strategy and is designed to increase security standards and cooperation among and between E.U. Member States.

This first deadline, by which Member States were required to "transpose" the Directive into respective national laws, fell on May 9, 2018. The EC updated its overview on the state-of-play of transposition for each Member State on its website. But another upcoming deadline could impact major companies operating in the E.U. By November 9, 2018, Member States must identify operators of essential services – i.e., private businesses or public entities operating in critical sectors that will have to comply with cybersecurity requirements and notify national authorities of significant incidents.

The NIS Directive aims to raise levels of the overall security and resilience of network and information systems across the E.U. According to the EC, the Directive has three main objectives:

1. improving national cybersecurity capabilities;
2. building cooperation at the E.U. level; and
3. promoting a culture of risk management and incident reporting among key economic actors, notably operators of critical infrastructure and digital service providers.

The NIS Directive encourages adoption of specific standards to raise the bar of security across the board. It states that, "standardization of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards so as to ensure a high level of security of network and information systems at Union level. ENISA [The European Union Agency for Network and Information Security] should assist Member States through advice and guidelines." While stating that cybersecurity standards should be market-driven, the NIS Directive simultaneously advances specified standards selected by Member States as advised by ENISA.

See also "How Will the GDPR Affect Due Diligence?" (Mar. 14, 2018).

What Companies Are Impacted?

The NIS Directive applies to two categories of private-sector companies:

- first, "operators of essential services" (which in the U.S. are considered critical infrastructure operators) within the energy, transport, banking, financial market infrastructures, health, water, and digital infrastructure sectors (e.g., internet exchange points, domain name system service providers, and top-level domain name registries); and
- second, "digital service providers" that offer services within the E.U., such as online marketplaces, search engines, and cloud computing services. Certain smaller digital service providers are excluded from the Directive.

Like the GDPR, the NIS Directive may apply to U.S. organizations doing business in the E.U. It will apply to E.U.-based subsidiaries of critical infrastructure operators as well as U.S.-based e-commerce and cloud computing companies.

Penalties for non-compliance are determined by Member States, and countries have contemplated stiff penalties, with some akin to those found in the GDPR.

See also "EY Global Data Analytics Survey Finds Lack of GDPR Preparedness and Need for Cross-Functional Collaboration" (Mar. 28, 2018).

What Are the Requirements?

The NIS Directive requires that certain security measures be implemented and for national authorities to be notified of significant cyber incidents.

With respect to operators of essential services, the security standard is risk-based: "Member States shall ensure that operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations." These operators shall "take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services[.]" Digital service providers should consider additional factors, including: "(a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing, and testing; and (e) compliance with international standards."

Notification obligations under the NIS Directive depend on certain factors, and notice must be given to national authorities "without undue delay." The significance of an incident impacting operators of essential services depends on: "(a) the number of users affected; (b) the duration of incident; and (c) the geographic spread." Digital service providers should also consider: "(d) the extent of the disruption of the functioning of the service; and (e) the impact on economic and societal activities." More structured reporting requirements are expected to be developed as Member States adopt and implement the Directive.

See also "A Practical Look at the GDPR's Data Breach Notification Provision" (Jan. 17, 2018).

Part of a Broader Trend in Europe

The NIS Directive grants ENISA broad authorities to help shape requirements in the Directive. The Directive establishes a "Cooperation Group, composed of representatives of Member States, the Commission, and [ENISA] to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems." According to ENISA, under the Directive, the agency assists the Cooperation Group by:

- identifying good practices in the Member States regarding the implementation of the NIS directive;
- supporting the E.U.-wide cybersecurity incident reporting process, by developing thresholds, templates, and tools;
- agreeing on common approaches and procedures; and helping Member States to address common cybersecurity issues.

In this capacity, ENISA has developed publications on identification criteria, incident notification, and security requirements under the Directive. ENISA is also active in other areas, helping Member States to develop national cybersecurity strategies, conducting cyber exercises, and coordinating with Computer Security Incident Response Teams.

The E.U. is not only expanding its privacy regime (through the GDPR) and security requirements for critical infrastructure operators and digital service providers (through the NIS Directive) – it also has connected devices, or the Internet of Things, in its sights.

In September 2017, the EC introduced a cybersecurity package, which includes a stringent certification scheme for connected devices. Under the Cybersecurity Act, the EC would establish rules to create certification schemes for particular Internet-connected devices and services. Presently, E.U. Member States have varied requirements, and this framework seeks to coalesce around a more uniform certification. Under the proposal, the certification schemes would be voluntary, "unless otherwise provided in Union legislation laying down security requirements [for] products and services." Among other proposals in the EC cyber package, a joint Commission and industry initiative would seek to define a "duty of care" principle to help reduce the risk of product and software vulnerabilities and promote "security by design."

Individual countries have provided voluntary IoT security guidance, which they threaten to make mandatory. The UK's Department for Digital, Culture, Media & Sport issued a report earlier this month, Secure by Design: Improving the cyber security of consumer Internet of Things. It says "[t]he Government's preference would be for the market to solve

this problem – the clear security guidelines we set out will be expected by consumers and delivered by IoT producers. But if this does not happen, and quickly, then we will look to make these guidelines compulsory through law. We will review progress throughout 2018."

See also "Lessons for Connected Devices From the FTC's Warning Against Unexpected Data Collection" (Feb. 22, 2017); "New NIST and DHS IoT Guidance Signal Regulatory Growth" (Nov. 30, 2016).

Looking Ahead

While the privacy and security implications and potentially massive penalties of the GDPR warrant companies' attention and resources, other European initiatives could have comparably large impacts on specific industries. The NIS Directive and efforts like the Cybersecurity Act are taking place with less fanfare. Critical infrastructure companies, digital service providers, and IoT device companies with services or operations in the E.U. should assess their cybersecurity practices and policies to ensure compliance with these new and expanding legal requirements.

More fundamentally, as the United States considers national strategies for cybersecurity, data privacy and IoT, it is imperative that U.S. industry and government engage international efforts and look at IoT security holistically, as a truly global issue. As market solutions emerge, U.S. companies should identify them to global standards groups and regulators. International collaboration here is critical to stave off fragmented or premature regulation that stifles innovation and global trade.

Megan L. Brown is a partner at Wiley Rein LLP. She is former counsel to the Attorney General at the U.S. Department of Justice, serves on the U.S. Chamber of Commerce Cybersecurity Leadership Council, and is a 2018 fellow at George Mason University's National Security Institute. She is co-author of pivotal IoT Security Report by the U.S. Chamber of Commerce.

Matthew J. Gardner is of counsel at the firm and a former assistant U.S. attorney.

Michael L. Diakiwski is an attorney at the firm and former counsel to the secretary and the general counsel of the U.S. Department of Homeland Security.