WILMERHALE

EU Cybersecurity Directive Brings Notification and Security Requirements for Industry

JULY 7, 2016

The first European Union-wide rules on cybersecurity have been adopted by the European Parliament. Approved on July 6, 2016, the Directive on Security of Network and Information Systems (NIS Directive) creates new risk management and incident reporting obligations for both digital service providers and operators of essential services such as banking or transportation. It also aims to improve national cybersecurity capabilities within EU Member States and to increase cybersecurity cooperation across the EU.

Improved National Cybersecurity Capabilities

First, Member States are directed to establish and adopt national cybersecurity strategies, which will define strategic objectives and lay out any appropriate policy and regulatory measures needed to achieve "a high level of security." Member States will be required to designate one or more national authorities to monitor application of the NIS Directive at the national level and designate a point-of-contact to facilitate cross-border cooperation with other Member States and within new cooperation mechanisms created by the Directive itself.

The NIS Directive also creates a network of "Computer Security Incident Response Teams" (CSIRTs) in each Member State to react to cyber threats and incidents. Each Member State will designate a CSIRT that will be responsible for:

- monitoring incidents at a national level;
- providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
- responding to incidents;
- providing dynamic risk and incident analysis and situational awareness; and
- participating in larger CSIRT networks.

Annex I of the Directive further explains that CSIRTs will work to establish a cooperative relationship with the private sector, and they will promote standardization practices for: (1) incident and risk handling procedures; and (2) incident, risk and information classification schemes.

Increased Cooperation across the European Union

In order to facilitate strategic cooperation and information exchange, the Directive establishes a "Cooperation Group" composed of representatives from Member States, the European Commission, and the European Union Agency for Network and Information Security (ENISA). The group is charged with establishing biennial Work Programs that can provide guidance to CSIRTs, assist in cybersecurity capacity building, and share best practices and information with respect to cyber risks, incidents and training.

The NIS Directive also creates a "CSIRTs Network" made up of national CSIRTs and CERT-EU. The Directive puts forward a number of responsibilities for this CSIRTs Network, including:

- exchanging information on CSIRTs services, operations and cooperation capabilities;
- exchanging and discussing information related to incidents (on request and voluntary);
- identifying a coordinated response to an incident (on request and voluntary);
- support cross-border incident handling (voluntary);
- exploring further forms of operational cooperation;
- informing the Cooperation Group of its activities and requesting guidance;
- discussing lessons learned from NIS exercises;
- discussing issues relating to an individual CSIRT (on request); and
- issuing guidelines on operational cooperation.

New Obligations for "Operators of Essential Services" and "Digital Service Providers"

Finally, the NIS Directive places obligations on businesses that are classified as operators of essential services or digital service providers.
The Directive does not explicitly define what an essential service operator is, leaving it to Member States to identify potential operators based on whether: (1) the entity provides a service that is essential for the maintenance of critical societal and economic activities; (2) the provision of that service is dependent upon networks and information systems; and (3) a security incident would have a significant disruptive effect on the provision of service. Operators of essential services will include companies within the following industries:

- energy;
- transportation;
- banking;
- financial market infrastructure;
- health;
- drinking water supply and distribution; and
- digital infrastructure, including Internet exchange points, DNS service providers and domain name registries.

Meanwhile, digital service providers are defined in Annex III of the Directive to include online marketplaces, cloud computing services and search engines. While any entity falling within these categories is automatically subject to the new cybersecurity and notification requirements, small and micro-sized enterprises are outside of the Directive's scope.

Both business categories will be required to put in place appropriate security measures, and for certain serious cyber incidents, to notify relevant national authorities. However, the NIS Directive does not define what constitutes a significant incident requiring notification, directing companies to take into consideration factors including the number of users affected, the duration of the incident, and its geographic spread.

Further, the NIS Directive recognizes that “the degree of risk for operators of essential services...is higher than for digital service providers.” As a result, the Directive envisions “lighter” security and notification requirements for digital service providers. While Member States are given broad purview over essential service operators, in order to ensure a “light-touch and harmonized approach" to regulating digital service providers, the European Commission itself is directed to establish security and notification requirements and Member States are prohibited from imposing more stringent rules. In general, digital service providers will need to take into account:

- the security of systems and facilities;
- incident handling;
- business continuity management;
- monitoring, auditing and testing; and
- compliance with international standards.

Finally, the Directive also encourages businesses outside of these two broad categories to notify authorities on a voluntary basis. A voluntary notice will not impose any obligations on that company to which it would not have been subject had it not provided notification.

What’s Next?

The NIS Directive enters into force in August 2016, and Member States will have until May 2018 to transpose its requirements into national law. Member States will then be required to identify essential service operators by November 2018. Penalties for infringing national provisions are instructed to be “effective, proportionate and dissuasive.”