KING & SPALDING

Client Alert

Corporate Practice

February 22, 2013

European Commission Publishes Cybersecurity Strategy and a Proposed Directive on Network and Information Security that Would Impose Significant Regulation of Industry

On 7 February 2013, the European Commission published two cybersecurity documents designed to provide a comprehensive vision of how European Union Member States, national authorities, and private industry will prevent and respond to cyber disruptions and attacks. The Cybersecurity Strategy is aimed at harmonizing national authorities of EU Member States to improve cyber resilience and reduce cybercrime while advancing cyberdefence policy and industrial and technical resources for cybersecurity. The European Commission has concluded that the current "voluntary approach" governing private market participants' responses to cyber incidents is no longer acceptable and has resolved, through an impact assessment, that a regulatory regime is necessary in specific critical sectors. The proposed Directive on Network and Information Security, if implemented, would impose significant regulatory hurdles on a host of private entities, including providers of banking, energy, transport, health, Internet, social media, e-commerce, and cloud computing services.

Overview of the European Commission's Cybersecurity Strategy

To safeguard an online environment with both freedom and security, the Cybersecurity Strategy is focused on five strategic priorities:

(i) achieving cyber resilience;

(ii) drastically reducing cybercrime;

(iii) developing cyberdefence policy;

(iv) developing industrial and technical resources; and

(v) establishing a coherent international cyberspace policy for the EU.

Many of these priorities are meant to be furthered through the proposed legislation in the Directive discussed below, which will set certain minimum requirements and also impose a regulatory structure across many industries.

A central focus of the strategy is increased cohesion between EU Member States to improve coordinated prevention, detection, mitigation and response mechanisms and improve information sharing and assistance between EU authorities.

Of interest is that the EU intends to promote a "single market" for cybersecurity products that focuses on the entire supply chain. It appears that this will mean additional "appropriate cybersecurity performance requirements" must be used across Europe, including labeling requirements and increased cooperation and

For more information, contact:

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

Pulina Whitaker
+44 20 7551 7586
pwhitaker@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

London
125 Old Broad Street
London, EC2N 1AR
Tel: +44 20 7551 7500
Fax: +44 20 7551 7575

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

transparency about security and the obligations on private industry set forth in the Directive. The European Commission also focused on developing uniform security standards for certifications in the area of cloud computing and on providing research and development incentives to "boost the internal market and reduce European dependence on foreign technologies". Finally, the EU will attempt to develop "a coherent EU international cyberspace policy" to allow increased international engagement, though there is currently no call for new international legal instruments for cyber issues.

The Proposed European Parliament and Council Directive Concerning Network and Information Security

A key component of the Cybersecurity Strategy is the adoption of a proposed Directive governing network and information security. The driving force behind the Directive is the view that the current voluntary measures undertaken by public authorities and market participants do not provide sufficient protection against cyber incidents and risks across the EU. The resulting "uncoordinated regulatory interventions, incoherent strategies and divergent standards" lead to insufficient protection of network and information systems and potential market barriers. The Directive's objectives are threefold:

- Requiring all EU Member States to ensure that they have in place a minimum level of national capabilities by establishing competent authorities for network and information security, setting up Computer Emergency Response Teams, and adopting national strategies and cooperation plans;
- Once established, requiring national competent authorities to cooperate within a network enabling effective coordination in the areas of information exchange and detection and response to cyber incidents; and
- Instituting a regulatory regime to require private market operators in specific critical sectors and public administrations to share information on regulatory incidents, assess risks, and adopt appropriate and proportionate measures to ensure network and information security, including through mandatory reporting of cyber incidents.

Much of the proposed Directive is therefore focused on greater coordination among, and harmonization standards and capabilities of, EU Member States. The Directive applies to all "market operators", meaning two classes of private entities:

- providers of "information society services" including e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services and application stores; and
- operators of critical infrastructure in the fields of energy, transport, banking stock exchanges, and health.

Modeled on the requirements applicable to telecommunications companies, the Directive will require market operators to "take appropriate technical and organizational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations … [that] shall guarantee a level of security appropriate to the risk presented." In addition, Member States will be required to ensure that market operators "notify the competent authority [of] incidents having a significant impact on the security of the core services they provide." The European Commission is empowered to define through implementing acts the mandatory notification procedures, which presumably includes the power to define the threshold to require reporting. The scope of this standard is unclear given that the key trigger—a "significant impact"—is undefined. The competent authorities are empowered either to inform the public or require the market operators to inform the public where it is in the public interest to do so. Additional guidelines and implementation standards are likely to follow from the European Commission or competent authorities. Key criticisms of the Cybersecurity Strategy are that the proposals could lead to a significant increase in notifications, over-burdening data protection authorities and businesses across Europe. The proposed directive could also conflict and overlap with the proposed new Data Protection Regulation which (in the current draft) will require businesses to notify the data protection authority of a data breach within 24 hours of becoming aware of it.

The Directive requires Member States to provide competent authorities within their jurisdictions with "all the powers necessary to investigate" non-compliance by market operators with their obligations. This includes requiring market operators to: "provide information needed to access the security of their networks and information systems, including documented security procedures;" and "undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority." In addition, competent authorities are to have the power to issue "binding instructions to market operators" and competent authorities will be required to coordinate with law enforcement where criminal activity is suspected and to cooperate with personal data authorities concerning incidents resulting in personal data breaches.

Next Steps

With the Cybersecurity Strategy in place, the European Parliament will consider the proposed legislation. Once enacted and published in the *Official Journal of the European Union*, the Directive provides that it will enter into force twenty days later. A series of implementing measures will then occur before private market operators are subject to new regulatory hurdles. The Directive defines the circumstances under which required notifications of cyber incidents will occur and, at that point, competent authorities within the Member States may adopt additional guidelines and issue instructions concerning incident reporting.

Recommendations

The proposed Directive on improving network and information security will pose significant compliance and regulatory hurdles to a broad cross-section of the business community. Particularly for those companies operating in one or more Member States in the banking, energy, transport, health, Internet, and social media industries, the process by which Member States implement this Directive will raise even more questions. Understanding these new policies and monitoring future developments will enable companies to prepare for further changes.

If you have any questions regarding the European Commission's Cybersecurity Strategy or the Proposed Network and Information Security Directive or related issues, please contact Pulina Whitaker at +44 20 7551 7586, Phyllis Sumner at +1 404 572 4799 or Alexander Haas at +1 202 626 5502.