LOS ANGELES
Daily Journal
www.dailyjournal.com
THURSDAY, APRIL 10, 2014
PERSPECTIVE

Attempt to harmonize European cybersecurity laws has flaws

By Grant Davis-Denny

The European Parliament recently passed a draft directive titled the Network and Information Security Directive. Although the NIS directive aims to harmonize cybersecurity requirements across the 27 European Union member states, the directive — if approved — has the potential to produce over two dozen country-specific laws with widely varying requirements. For U.S. companies operating in Europe that are already grappling with complex cybersecurity regulations domestically, the cybersecurity landscape is likely to become more, not less, complex in the coming years.

Three Key Provisions for Businesses Operating in Europe

In its current form, the NIS directive applies to certain businesses providing services in Europe that operate in the energy, transportation, banking, financial market infrastructure, Internet exchange points, food supply chain and health sectors. The directive's provisions would apply to businesses in these sectors where the disruption or destruction of the business's network would have a significant impact on an EU member state.

For covered businesses, the directive has three key components:

Cybersecurity Standards: EU member states must require covered businesses to "take appropriate and proportionate technical and organizational measures to detect and effectively manage the risks posed" to their networks' security. The directive does not specify the steps that companies must take to protect their networks. It broadly suggests, however, that security measures must be state of the art, address prevention and mitigation, and ensure continuity of a business's core services.

Incident Reporting: The 27 member states are required to ensure that covered businesses notify regulators of cybersecurity incidents "having a significant impact on the continuity of the core services they provide." Significance of impact depends on the number of users affected, the incident's duration, and the incident's geographic scope.

Evidence of Effective Security Policies: Member states also must grant their regulators the authority to mandate that covered businesses provide evidence that they have effectively implemented security policies, such as a security audit conducted by an independent body or regulator.

Complicating, Not Simplifying, Compliance

In proposing the directive to the European Parliament, the European Commission warned: "Divergencies in NIS regulations represent a barrier to companies wanting to operate in several countries and to the achievement of global economies of scale."

This concern is well-placed. The burdens of complying with 27 different cybersecurity laws would be significant.

But for several reasons, the directive is unlikely to simplify the cybersecurity landscape in Europe:

Floor, Not a Ceiling: Although the directive sets an EU-wide floor for cybersecurity laws, it does not set a ceiling. Member states thus are free to adopt more stringent requirements than those in the directive.

Binding Results, but Nonbinding Methods: By their nature, EU directives are not designed to produce uniform standards. Instead, directives specify a result to be achieved, but leave to each member state the choice of method to achieve that result.

Vague Standards in the NIS Directive: The directive's provisions lack detail and are ambiguous. For example, the directive vaguely requires that a covered company's cybersecurity measures be "appropriate and proportionate." This ambiguous phrase affords enormous discretion to drafters of cybersecurity standards.

A Laundry-List of Regulatory Possibilities: The number of potential cybersecurity requirements that EU member states could impose is substantial. In February, the National Institute of Standards and Technology, a U.S. agency, released its cybersecurity framework. NIST's framework contains a list of nearly 100 high-level categories of security policy, such as "Remote access is managed." Within each of these categories, a plethora of policy choices could be made. In the remote access management example, an EU member state might set criteria for user authentication technology, place limits on remote access by vendors, or restrict employee access while traveling abroad. If each of the 27 EU member states responded to the directive by selecting their own approaches to hundreds of cybersecurity issues, it is not hard to imagine the regulatory nightmare that the directive could spawn.

> For U.S. companies operating in Europe ... the cybersecurity landscape is likely to become more, not less, complex in the coming years.

Prospects for Harmonization: Although the directive purports to encourage harmonization of EU member states' cybersecurity laws, there is reason for skepticism that it will achieve this result.

For one, the directive grants individual member states, not the commission, the authority to determine whether a company's services are critical enough that the company should be regulated.

Moreover, the commission's rulemaking authority does not extend to the ability of member states to seek production of a company's security policies. Each member state thus is free to determine what evidence it believes a covered company will need to produce to satisfy regulators that the company has "effective" cybersecurity policies in place. Worse yet, under the directive each member state may decide on its own whether a covered company should be subject to additional cybersecurity audits.

While the directive requires each member state's regulator to work with the European Network and Information Security Agency to develop consistent "sector-specific" guidelines for data-breach notification events, the directive also grants individual member states the right to adopt their own guidelines on when notifications must be made.

Finally, under the directive, member states must encourage, but need not require, companies to follow a list of cybersecurity standards that are to be drafted by an unspecified European standardization body to be chosen by the European Commission. Whatever standards may make it onto this list, the directive expressly allows member states to adopt more aggressive requirements for covered companies.

Next Steps for the NIS Directive

The draft NIS directive now goes to the European Council of Ministers for approval. If the council adopts the directive without amendment, member states will have 18 months to adopt and implement the cybersecurity standards, reporting requirements, and auditing provisions in the directive.

Grant Davis-Denny *is a partner at Munger, Tolles & Olson LLP in Los Angeles. He can be reached at Grant.Davis-Denny@mto.com.*

GRANT DAVIS-DENNY
Munger, Tolles & Olson