Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Things To Watch As EU Cybersecurity Directive Looms

By **Melissa Lipman**

Law360, New York (July 6, 2017, 1:31 PM EDT) -- European Union nations have less than a year left to put in place new cybersecurity rules designed to protect key industries like banking, energy and technology from attacks.

The EU Network Infrastructure Security Directive is designed to set minimum blocwide standards to prevent cyber breaches — and to tackle problems once they happen. It also calls for penalties set at the national level for firms that either don't have enough security protections or that fail to notify authorities of any incidents.

While much of the burden falls on national governments to set up cybersecurity agency, framework and response systems, the national laws transposing the EU legislation will also create new burdens for companies to ensure they have state-of-the-art protections in place and to report breaches.

Though national governments will create lists of the companies that must comply, certain sectors can already expect to face new requirements: banks, securities exchanges, energy firms, healthcare providers, water systems and technology giants.

Here are five things companies facing the new rules should be watching as the EU's 28 national governments start working on new rules for May 2018.

The Lists of Who Must Comply

The legislation is what is known as a minimum harmonizing directive under EU law. Essentially, it sets out a broad framework for what countries have to do, but national governments will have considerable latitude to decide which firms must comply, what companies actually have to do and what the repercussions will be for failing to meet those standards.

The directive itself lays out two groups of companies that will have to report security incidents: essential service providers and digital service providers. Though the companies likely to be affected can take an educated guess about their status — banks, stock exchanges, electric grids and cloud providers are unlikely to escape attention — the final lists set by national governments aren't due until November.

"These organizations have got to get ready to make sure they're going to comply with a minimum set of requirements and have processes in place for notifying these set of teams when breach takes place,"

said Mayer Brown International LLP's Oliver Yaros. "Certainly in the U.K. there hasn't been that much coverage of what the government is going to do [and] they haven't commented on who is going to be on the list as yet."

While many companies can likely assume they'll be on the list, even those unlikely to be added should be paying attention to how the directive gets implemented at the national level, according Paris-based Gibson Dunn & Crutcher LLPpartner Ahmed Baladi.

"Although the directive is targeting specific categories of entity, everyone should feel a concern across the sectors," Baladi said "You could be an entity which is not part of a list of categories … but could do business with any of those entities and therefore you [would be] also interested in knowing to what extent this provider or partner will be subject to national law transposing the EU directive."

For example, a company relying on a cloud computing provider that has to notify government authorities of a security breach could well face its own public relations crisis if its own customers know their data could have been affected by a hack, Baladi said.

At the same time, experts say that companies in regulated industries like financial services may face more limited additional burdens to comply with the new rules. Instead, the cybersecurity directive would likely hit technology firms and infrastructure providers the hardest.

"If you're a nonregulated entity and you don't have much of an online presence but do have important IT infrastructure, a water supplier or something like that, then perhaps this is going to be a more serious challenge for you," Yaros said.

The Directive's Overlap With Data Protection Rules

The cybersecurity directive is separate from the new General Data Protection Regulation that takes effect in May, but in practice experts say it was hard to imagine too many scenarios where a cybersecurity incident wouldn't also involve personal data.

"All organizations should be taking quite a serious look at what security measures they have in place to prevent cyberattacks because … I don't think that not being on the list means you are expected by the government to have a lesser degree of protection, particularly where you're protecting personal data," Yaros said.

There are some similarities between the two regimes: Both require firms to take steps to protect data or systems, both require similar notifications to national authorities and both impose similar time limits for coming forward.

"If you believe you're taking appropriate measures under the GDPR, perhaps that will be good enough for the NIS directive," Yaros said. "But the NIS directive is likely to have more specific requirements about how you secure data than the GDPR does."

Though the standards may vary from country to country, the directive calls for firms to have state-of-the-art measures in place to prevent attacks and protect infrastructure.

But even though the frameworks are similar, the dual notification requirements almost certainly mean companies facing an attack will have to deal with two parallel processes. And until more details of the

national laws come out, it remains unclear if national data protection agencies and national cybersecurity authorities will work together on breaches that run into both measures.

"The risk that I see is that I'm not sure that the two authorities will have the same approach in handling the situation," Baladi said. "Under the GDPR, I could imagine under specific conditions you have to report the data breach to the individuals whose data has been lost or hacked. I don't know how a national security agency would react."

The result could be one authority telling a bank it need not inform its clients of lost data, and another that orders disclosure. And in the case of regulated sectors, like banking, the company may have to factor in the position that the industry watchdog takes as well, Baladi said.

"If one of my clients were calling me and said, 'We have an issue and we've been hacked,' I'd of course advise them to check the impact of the attack on their activities and data and to what extent they have to report to the authorities," Baladi said. "But in any case, when I will have my client report that to the data protection authority, I will also advise them to mention they had to report same incident to the cybersecurity agency, and to strongly invite them to cooperate."

The Size of the Penalties

One of the most attention-grabbing aspects of the new data protection rules is that they empower national authorities to hand out potentially massive fines: €20 million ($22.8 million) or up to 4 percent of the company's annual global turnover — whichever figure is greater.

But the cybersecurity directive comes with penalties, too. The problem at the moment is that it's unclear at what level each national government will set potential fines.

"The EU directive provides that the member states should define the rules on the penalties, which would be applicable for violations of national provisions," Baladi said. "What the EU directive wants is to make sure member states will put in place penalties, and directive says they should be effective, proportionate and dissuasive."

The fines will almost certainly be lower for the cybersecurity directive. In Germany, for example, failure to comply with security standards or notification requirements could lead to administrative fines of up to 100,000, according to Jones Day partner Undine von Diemar. At the same time, companies could be facing those kinds of penalties on top of any sanctions for data protection violations.

"There's going to be enforcement in both areas," von Diemar said. "Okay, maybe [the NIS fines are] less, but … in most cases you will have a data breach anyway and if you don't report a data breach, that's really the relevant factor in terms of the fine that can happen."

Beyond the penalties themselves, however, companies that fail to comply with the cybersecurity directive's state-of-the-art protections mandate could also face other liabilities, according to Baladi.

"The other concern you can have is to be subject to some claims by the victims … which would consider, 'If you had implemented that state-of-the-art measure, maybe the consequences would have been different and my risk or my damages would have been different,'" Baladi said.

That threat of litigation, which already exists with breaches, could become worse with a new set of EU

standards companies have to meet. The result is that it will become all the more important for businesses to make sure they live up to whatever national laws end up considering state-of-the-art protections to be, he said.

The Toughest Enforcer in the Bloc

Unlike the GDPR, which sets exact rules for the entire EU, the cybersecurity directive offers relatively little in the way of blocwide guidance.

"Beyond setting up a mechanism for breach notifications and beyond setting up a minimum set of standards and creating a framework for reporting and dealing with incidents, it's not too clear what the directive is going to require in each jurisdiction," Yaros said. "It's drafted in quite a general way."

And even though a hack might only affect a data center housed in Germany, the effects of that incident could ripple across the EU if the company has customers based in other nations, implicating several different cybersecurity regimes.

Still, even though the directive leaves significant room for each nation to set its own rules, in reality companies affected will have to meet the bar set by whichever EU country takes the toughest approach.

So far, Germany, which already had cybersecurity legislation in place, has made the necessary changes to transpose the directive, but it remains an open question what approach to penalties and standards the rest of the bloc will opt for, according to von Diemar.

"You can't apply different IT security standards, usually, varying country by country. That's not the way you would organize a digital business," von Diemar said. "Practically, it means that the strictest standards will need to be adhered to."

The International Ripples

Just as a company based in one EU nation may need to contend with other cybersecurity regimes across the bloc, firms that are physically based entirely outside of the EU may still find themselves caught up by the new directive.

That's because the directive has an extraterritorial reach, much like the data protection regulation, when EU customers are affected, von Diemar said.

That could be a particular threat to companies that offer cloud computing services, who can easily reach across national borders.

"I worry more about digital service providers, especially those located outside of the EU, as this really has an extraterritorial scope," von Diemar said. "So if a cloud computing company sits outside the EU, it can nevertheless be caught, when it offers services within the EU."

--Editing by Rebecca Flanagan.