Endpoint Security , Geo-Specific , Internet of Things Security

Europe Girds for Looming IoT Security Regulations

European Commission Publishes Draft Guidance for Cyber Resilience Act

David Meyer • March 27, 2026

Image: Shutterstock

Key implementation deadlines loom for one of Europe's most consequential cybersecurity laws and draft guidance from the European Union may help manufacturers comply - up to a point.

See Also: The Healthcare CISO's Guide to Medical IoT Security

The Cyber Resilience Act is an expansive law approved in 2024 that will introduce security requirements for all manner of internet-connected "digital products," from smart fridges and phones to apps, enterprise software and even some cloud services.

Much as the EU General Data Protection Regulation influenced how companies handle data around the world, the CRA will force security-first design choices on any company that wants to sell its digital products in the European single market. Serious cybersecurity assessments and protections will become essential to receiving that crucial "CE" mark of conformity, without which European importers and retailers won't be able to touch the products.

Starting in December 2027, manufacturers will have to provide timely security updates for their connected devices and software, the design of which will require supply-chain risk assessments and the implementation of measures such as data protection by default. The nearest deadline comes this September, when manufacturers will have to start reporting actively exploited vulnerabilities and certain other severe security incidents to ENISA, the EU Agency for Cybersecurity. In general, national market surveillance authorities will police CRA compliance.

When the CRA passed, companies had a lot of questions. Would open-source software projects suddenly be saddled with burdensome compliance requirements? The regulation says products must receive security updates for at least five years. What about particularly long-lasting or ephemeral products? Which cloud services fall under the CRA's scope? The regulation calls for disclosing most vulnerabilities within 24 hours, but 24 hours from when exactly?

Earlier this month, the European Commission published draft guidance for implementing the CRA. Manufacturers, developers and others have until April 13 to provide comments. According to Ceyhun Pehlivan, a Madrid-based lawyer who has been advising companies in their scramble to meet the CRA deadlines, there's a lot to like in the guidance - but also a few issues that will likely remain challenging.

"I think it is a strong first step. It answers many practical questions companies had," Pehlivan, also an adjunct professor at IE Law School. "But it also shows that some of the hardest issues, like software updates and cloud dependencies, are inherently difficult to regulate cleanly in practice," he told Information Security Media Group.

On the plus side, Pehlivan said, the draft guidance does a good job of helping companies understand which products fall under the CRA's scope, a particularly concerning issue when it comes to software, which sometimes doesn't map neatly to previous conceptions of EU product law. The draft specifies that software appears on the European market as soon as it is made available for download or remote access there. Providing sample or demo code for demonstration purposes doesn't count. Hardware and software products fall outside the CRA's scope if they don't have a network connection.

The proposed guidance also clears up some confusion around which cloud or SaaS elements of products are covered by the CRA, by introducing a three-question test for determining if they qualify as so-called remote data processing solutions. If they don't process data "at a distance" then fall outside the scope. If they do, but the product wouldn't lose core functionality in their

absence, then they also aren't remote data processing solutions but must be treated as a component, meaning the manufacturer must do due diligence. Ditto if they are needed for core functionality but the manufacturer didn't design them, or isn't responsible for them.

"Basically, if you translate that, your own back-end is likely to be covered," said Pehlivan, explaining that the likes of Amazon Web Services would typically be treated as a component. But he also warned that aspects of modern software architecture such as microservices and APIs might make it difficult to apply the remote data processing solution test. "Real-world architectures don't always fit into these categories that the European Commission proposes," he said.

The CRA's implications for open-source projects are particularly thorny, at least for anyone trying to commercialize the software - and that community had been keenly awaiting what the commission's draft guidance.

The draft guidance says that contributors of source code have nothing to worry about, as long as they don't "control releases, roadmaps, or governance decisions." Manufacturers trigger the CRA's requirements when they charge for their open-source software - or require the processing of personal data as a condition for use - but the free version of the same software is not technically placed on the market and therefore escapes the law. Anyone who gives away the software and charges for its support but also allows users to go elsewhere for support are likewise outside from the CRA's jurisdiction.

The Open Regulatory Compliance Working Group, a body that advocates for the open-source sector, responded to the draft guidance with cautious enthusiasm. "The European Commission has demonstrated that it is listening to well-founded input from technical communities," wrote Juan Rico, an ORC senior manager and Eclipse Foundation employee. Rico also said there were "still areas where clarification and improvement would benefit both regulators and the broader ecosystem."

Pehlivan said the draft regulations still create the potential of legal uncertainty for open-source projects.

The lawyer also sees trouble ahead for software vendors who make significant changes to their products via updates. Making "substantial modifications" that change the product's intended purpose, or affect "the product's compliance with the essential cybersecurity requirements," essentially qualifies under the CRA as placing a new product on the market.

"Even limited or seemingly minor new functionalities may introduce significant cybersecurity risks, if such risks were not included in the original risk assessment and may impact compliance with the essential requirements," the draft guidance reads. "The assessment of substantial modification should therefore not be based on the scale or complexity of the change, but on its potential effect on the product's cybersecurity risk profile."

According to Pehlivan, companies could face issues when deciding whether an app update constitutes a "substantial modification" or not. "The company could argue that it was not, but the supervisory authority can say it is substantial, so this is going to be up to the authority to decide," he said. "This is one of the gray areas that still remain."

As for the other burning CRA questions, the draft guidance provides significant clarity.

Importantly for the upcoming reporting deadline in September, companies now know that they will probably have to notify ENISA and their national computer security incident response teams within 24 hours of becoming aware of an actively exploited vulnerability. The clock isn't delayed to when they confirm the vulnerability.

Regarding support periods, the draft says five years is just a floor. If the product is supposed to last significantly longer, it should get security updates for a correspondingly longer period. It also aims to calm the nerves of companies putting out products that are supposed to last significantly less than five years, saying the minimum support period is just a "safeguard" and "a support period of five years is... not to be considered as the default for all products."

Either way, manufacturers will need to inform customers, at the time of purchase, of the end date of the support period - "at least" down to the month and year - and even to "display a notification to users once the support period expires, where this is technically feasible."

"If you think about enterprise software, usually the lifecycle is longer than advertised, so companies cannot really arbitrarily pick five years if their users are going to rely on the product, in practice, longer than that," said Pehlivan, who categorized this as another remaining gray area because it is often "hard to predict the real usage of the product."

About the Author

David Meyer

freelance writer

David Meyer is a freelance technology journalist based in Berlin. He previously was a senior writer for Fortune, covering artificial intelligence. He has worked for Politico Europe and written for ZDNet, Privacy Advisory and the BBC.