



Subscribe



How the EU Cyber Resilience Act could impact CIOs

By [Mark Chillingworth](#) September 12, 2023

Audio mode

Dyslexia mode

SUMMARY: Open source communities concerned by the EU's new Cyber Resilience regulations and CIOs need to be aware of the impact

Europe's Cyber Resilience Act will regulate open source software. In some quarters of the technology industry, new regulations from the European Commission (the operational arm of the European Union) spark hyperbole and levels of fear that the overseas press barons of the UK's mass media would be proud of.

European regulation, whether it be the mythical straight bananas or open source code, always stirs up emotions and heated debate, but what is the real impact on open source and what do CIOs and CTOs need to be aware of? With no tax-avoiding press barons to answer to, diginomica set out to discover whether the Cyber Resilience Act will deliver clean and safe beaches, or be a behemoth of damage like the Common Agricultural Policy.

[Announced back in September 2021](#), Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age, said at the time:

" *It will put the responsibility where it belongs, with those that place the products on the market.*

Four pillars are proposed:

- rules for products with digital elements to ensure their cybersecurity;
- essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products;
- essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle. Manufacturers will also have to report actively exploited vulnerabilities and incidents;
- rules on market surveillance and enforcement.



(© Rawpixel.com - Shutterstock)

Subscribe To Our FREE Newsletter

Of these pillars, the need for 'Manufacturers to report actively exploited vulnerabilities and incidents' has sparked the most fear. The initial proposal said technology providers had to report vulnerabilities to the EU agency for cybersecurity (ENISA), which was going to build a single reporting platform. Mike Milinkovich, Executive Director of the Eclipse Foundation was especially concerned by this:

" *That runs completely counter to accepted cyber security practices, where you keep an unfixed vulnerability confidential and you only talk to the people that can fix the vulnerability. Then, there is a coordinated disclosure process to make the vulnerability and the fix available all at once.*

There are two things with providing information on an unfixed vulnerability to government agencies. One, it provides a database of unfixed vulnerabilities, which is like catnip to hackers as it is such an attractive target. Secondly, governments are not always benevolent actors, and all the security agencies of the EU states would have access to this database for their own clever machinations.

The Eclipse Foundation counts enterprise technology suppliers Microsoft, Oracle, SAP, IBM, Fujitsu, Red Hat and Huawei as members, as well as corporations such as Bosch, Mercedes Benz and the European Space Agency and is a not-for-profit body for open source software.

On July 19, Carme Artigas Brugal, State Secretary for digitalization and artificial intelligence, released a statement, which detailed that following a review, the Cyber Resilience Act would instead demand that vulnerabilities or incidents be reported to the 'competent national authorities computer security incident response teams'. In other words, that's national bodies rather than the single body for the member states of the European Union.

Negative impact

Vulnerability reporting is only one concern that the open source community has towards the Cyber Resilience Act. Kim Sneum Madsen, CEO of Danish open source digital experience application provider Umbraco, says:

" *The ecosystem and supply chain of future open source technology products could become a concern.*

The EU-based CEO raises a valid point: the technology sector is famous for innovations coming from small garages or corners of academia. But equally, for enterprise CIOs and CTOs, there is always a need for innovative technology to be able to match the scale of the enterprise. Umbraco itself recently acquired an ecommerce business that had great technology but could not win customers of a certain size, but that is no longer the case as part of Umbraco.

The Cyber Resilience Act intends to place the CE mark responsibilities with open source foundations, which Olaf Kolkman, Principal at the Internet Society, is concerned about:

" *One of my concerns was that a platform like Github could have a compliance role in software publishing. That would have a big effect on open source. And I wonder at the willingness of these platforms.*

The Eclipse Foundation worries that the CE mark requirements will place a burden on open source developers and providers. Milinkovich says:

" *The open source communities are going to have to document processes and patch processes after a release in order to get a CE mark for every release they do.*

There will be CIOs and CTOs in highly regulated sectors that will give a gallic shrug to this, as process documentation is part and parcel of daily life and product development in their vertical markets. There is, of course, the difference that open source is often just the foundations that a CIO's team can use to develop their own application, as Milinkovich says:

[Subscribe To Our FREE Newsletter](#)

" *Open source licences don't have a field of use attribution; an example is the Eclipse Foundation desktop development tools. People have used this to develop applications for the instruments on the International Space Station and the ground control software used by the European Space Agency.*

Closer to home than the International Space Station, OpenUK CEO Amanda Brock points out that open source software underpins the very digital landscape that Europe and all economies rely upon:

" *Every public cloud is built on open source. The hyperscalers all use open source, whether it is Kubernetes or an open stack.*

Brock and others are concerned not only by the language of the Cyber Resilience Act but also how Europe will implement the act. She says:

" *How will they manage the audits and certifications that are required? I don't think they understand the scale of what they are trying to do. It could take three to five years to appoint a body to make this work.*

Umbraco CTO Filip Bech-Larsen adds:

" *As with many of the EU regulations, the intentions are good, but the implementation will be by national authorities, and it is always they set out their implementation plans.*

Border controls

Inevitably, an EU proposal has stirred up some hype. Milinkovich says:

" *The consequences of the Cyber Resilience Act, if it includes these ill-advised regulations on open source, is that a lot of the open source ecosystem resides outside of Europe, and they will say 'you are not to use this software in Europe'.
Cutting off the global supply chain of open source code is a real possibility, and that is an unintended consequence that I don't think the authors anticipated.*

In the UK, a former member of the European Union, Brock agrees:

" *No one will take on the responsibility, so the act is cutting off their nose to spite their face.*

Will the technology industry really ignore a market of 27 nations with a gross domestic product (GDP) of €14.5 trillion? That is hard to believe. Those advocating ending trading relations with Europe may want to consider the findings of the Office for Budget Responsibility in the UK, which has found that productivity in the UK is down by four per cent, exports and imports are down by 15% and the few trade deals achieved have had 'no material impact'.

Regulating tech

Europe's Cyber Resilience Act is the first move in what is expected to be a wave of regulations coming to technology.

Milinkovich of the Eclipse Foundations says:

" *Every CIO and CTO needs to recognize that it is not just Europe; the USA is going to bring regulations into the technology industry. The software industry has grown up over the last 50 years and has been unre*

[Subscribe To Our FREE Newsletter](#)

That poses as much of a challenge to the regulators as it does to the producers of technology, which the development of the Cyber Resilience Act has highlighted. Brock at OpenUK says:

// *There is factually incorrect stuff, such as the way they categorize commercial and non-commercial, for example, all open source can be used commercially. It demonstrates a lack of understanding of how technology actually works.*

Milinkovich adds:

// *The people that wrote the act know nothing about technology or the economics of the technology industry. They are not rewarded for getting it right; they are rewarded for getting the act passed.*

For this reason, Kolkman at the Internet Society says the technology industry has to get involved with the amendment and advisory process of creating European law:

// *There are still the tripartite negotiations, so there will be an opportunity to shape the text and the outcome. Pay attention now to see how this affects your business and mobilise your community.*

My take

Like any state, organization, global body or senior leadership team, Europe can lay claim to good and bad policy. The development of the Cyber Resilience Act requires all parties of all sizes to get involved, and as CIOs and CTOs increasingly develop software solutions as part of the customer offering, they too will need to be involved.

Read more on: [Regulation](#) | [Public sector](#) | [Security](#) | [Audio](#)

Related Stories



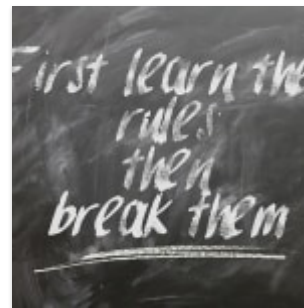
European Commission lays out plans for EU-wide Cyber Resilience Act to secure connected products



EU makes 'resilience' new compass for policy making as COVID-19 highlights vulnerabilities



Does the CIO need to understand technology? CASTing around for an answer to the 'how' of software



Uh oh, AI, EU - what could possibly go wrong? The risky business of regulation




UK puts 'Help us!' message in bottle at cybersecurity event

Powered by

Premier partner newsfeed

 **PURESTORAGE** Unleashing Possibility at the Gartner IT Symposium

 **CONFLUENT** Unlocks Vehicle Uptime & Supply Chain Visibility with Data Streaming

 **ASUG** How DTE Energy Leveraged SAP C4C Solutions to Revitalize Its Customer Reimbursement Program

[Subscribe To Our FREE Newsletter](#)



Climbing The Servitization Staircase Using Asset Data



Mastering Service Life Cycle Management: Key Strategies for Manufacturing Success



Sage Intacct 2023 Release 3 highlights: More industry enhancements to simplify and streamline your financial processes



Common Shipping Mistakes and How to Avoid Them



Inspiring Finance Leaders at Planful's User Groups



Workday Podcast DevTalk: How Workday and AWS Are Accelerating Innovation



Celonis Labs Beyond 2023: How GenAI, LLMs, process-centric IT and other innovations are shaping the future of process mining



Say hello to September integrations



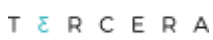
Are your sales and finance teams connected in the right way?



Generative AI Regulations – What They Could Mean For Your Business



Put GenAI to work in your industry



Introducing the 2023 Tercera 30: The top cloud ecosystems for partners



Josiah Davisson: Learning Java in High School



Samsara named as one of the UK's Best Workplace for Women™.

Latest Conversations

Sarah Lafferty:

That is a BRILLIANT headline!!!!

[Britannia waives the rules? The UK is a 'buccaneer' when it comes to tech regulation, claims Brexit leader](#) · 1 day ago

cliveb:

Larry Ellison gets it; AI ERP is all about orchestrating machine learning against big globs of operations data, not customer data. This requires privacy policy is properly sorted to protect...

[The "deep water of the Information Age" offers Oracle great opportunity, argues CTO Larry Ellison, but Wall Street takes a cool view of Q1 numbers](#) · 2 weeks ago

glawton:

Also if you feel so move to file a letter to the US Copyright Office, please post it here. Who knows, it

[Subscribe To Our FREE Newsletter](#)

glawton:

I just wrote my own letter to the Copyright Office about this matter. Please pile on if you agree, or add additional comments about other areas you feel are appropriate. Here is what I wrote: To...

[An important development - US regulators revisit copyright for AI](#) · 3 weeks ago

Jon Reed:

Indeed - well said. I think much of it comes down to proving that your BTP-based interfaces and extensions don't break from release to release and upgrade to upgrade (as long as your internal...

[On generative AI disruptions, RISE and GROW - Thomas Saueressig reveals the next steps in SAP's AI strategy](#) · 1 month ago

More on this topic



European Commission lays out plans for EU-wide Cyber Resilience Act to secure connected products



EU makes 'resilience' new compass for policy making as COVID-19 highlights vulnerabilities



Does the CIO need to understand technology? CASTing around for an answer to the 'how' of software

Go to topics

diginomica

diginomica and the diginomica logo are trademarks of diginomica Limited.

© DIGINOMICA LIMITED AND ITS LICENSORS 2013- 2023

[Cookie settings](#)

Developed by [BRAINSUM](#) .

[Subscribe To Our FREE Newsletter](#)