The European Union is a uniting of twenty-seven diverse nation states into one political union. This union ranges from the tip of the iberian peninsula to the Carpathians in Romania. Any expansive political bloc of this size consisting of this many sovereign nations will face many political hurdles in passing comprehensive legislation, that is the exact issue faced by the Cyber Resilience Act when it was first adopted. An adoption of this scale will face the issue of "patchwork" laws creating confusion among member states as pointed out here, "From a regulatory perspective, the European Union (EU) legal framework appears to be fragmented in relation to cybersecurity requirements for products with digital elements, as the various initiatives taken thus far at Union and member state level partially address the identified problems…..This creates legal uncertainty for both manufacturers and users while adding an unnecessary burden on market operators to comply with overlapping requirements for similar types of products." (Chiara P.G., 2022). One of the stated goals of this policy is a standardization, so this is a huge issue that needs to be addressed. Creating a minefield for producers is not a good way to ensure a positive reception to the policy. In Europe there is a rising wave of "EU skeptics" that are gaining traction and, much like comparable populist movements across the world, one of the core pillars is a staunch pro business anti regulation attitude. Granted that is a small wave but it bears mentioning, mostly these anti regulation arguments manifest as worries about policy overriding best practice, "Deficiencies also occur when policy mandates conflict with cybersecurity best practices. The European Union's

(E.U.’s) proposed Cyber Resilience Act includes a requirement that firms report the existence of a vulnerability to the government within 24 h of discovery; however, the development of a tested vulnerability patch typically requires a greater amount of time. Software vendors and security researchers are concerned about government organizations storing and protecting these cyber risks, which are referred to as zero-day vulnerabilities” (Hodgins, M.W. 2024). One of the key political balances is maintaining the goal of a policy while addressing fears of the professionals in the industry. Governments often lag behind industry and that is especially true in technology, so it can be a challenge to meet these demands when a policy like this can take years to get passed. The political reality is never exactly what experts or industry leaders want. On the ground floor of the council or when the policy is being written there are no experts there all of the time, so things will be left out. To the chagrin of many a computer whiz there were no special provisions for open source software when the policy first launched. As open source software is a community based decentralized effort it has been able to sail on mostly unregulated until the cyber resilience act. The layman would be remiss to imagine the world of open source software as a playground for hobbyists and of no real value when this is the one place where the utopian ideal of an egalitarian internet was realized with many advancements to boot, as a stake in the eye of tech giants. Operating systems like linux or web servers like Apache which are used far and wide are open source projects. Open source developers lodged this complaint, “The initial

version of the CRA drew sharp criticism from various entities, including over a dozen open-source industry bodies who wrote an open letter expressing concerns about its potential to stifle software development. The primary issue raised was the fear that upstream open-source developers could be held accountable for security flaws in downstream products, discouraging volunteers from contributing to OSS development or maintaining it due to fears of legal repercussions." (Liane Colonna. 2025). This was quickly addressed with revisions of the policy act but it shows that in this sort of political environment the crafting of effective policy can be a collaborative effort, "The revised legislation alleviates some of these concerns by providing exceptions for open-source projects and establishing separate roles and responsibilities for various actors in the software and hardware supply chain, including, for example, OSS contributors, OSS stewards and manufacturers." (Liane Colonna. 2025). The world of cyber security is not an island and cannot be separated from the political reality of passing legislation. It would be at the benefit for any cyber security professional to understand the political implications of every suggestion and be ready to defend best practices from poorly thought out regulations.

Chiara, P.G. The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. Int. Cybersecur. Law Rev. 3, 255–272 (2022). https://doi.org/10.1365/s43439-022-00067-6

Hodgins, M.W. The perils of cybersecurity regulation. *Rev Austrian Econ* **38**, 391–411 (2025). https://doi.org/10.1007/s11138-024-00660-4

Liane Colonna,

The end of open source? Regulating open source under the cyber resilience act and the new product liability directive,

Computer Law & Security Review,

Volume 56,

2025,

106105,

ISSN 2212-473X,

https://doi.org/10.1016/j.clsr.2024.106105.

(https://www.sciencedirect.com/science/article/pii/S0267364924001705)