DIGITAL RESILIENCE FORUM

SECURITY OF THE DIGITAL SUPPLY CHAIN

Daniel Izquierdo Cortázar

2025

SECURITY OF THE DIGITAL SUPPLY CHAIN

DIGITAL RESILIENCE FORUM

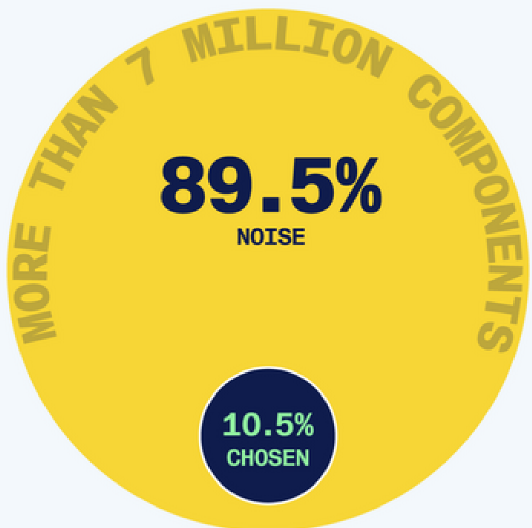
The Problem with the Digital Supply Chain

Various studies find that modern software applications are mostly made up of free software solutions. These percentages can rise to up to 90% of the total code, including dependencies. At the same time, most existing free software projects are not maintained. This is a troubling fact when it comes to securing software supply chains from attacks. That's why it is essential that organizations and European sectors work together to secure those software components that are key to a strong digital infrastructure.

As a powerful example of the issue, Maven Central, the largest repository of free Java software projects, has 85% of repositories that are unmaintained and inactive. Other data studies show that two-thirds of the dependencies written in Go of the Kubernetes project, a technology massively used by the industry, are at risk, mainly due to insufficient talent maintaining them. This lack of maintenance leads to a situation where most dependencies have added risks. The problem lies primarily in the second and third-level components, which are hierarchical dependencies of larger projects but are assumed to work.

FIGURE 3.4

Open Source Developer Choice



This pie chart shows developers' challenge when choosing among millions of components; nearly 90% will be noise.

[1] Free software is understood to be any software whose license has been approved by the Open Source Initiative and/or the Free Software Foundation. As an illustrative example, the Open Source Initiative's definition of free software is shared: https://opensource.org/osd

[2] A Summary of Census II: Open Source Software Applications Libraries the World Depends On. The LInux Foundation. https://www.linuxfoundation.org/blog/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on

[3] https://www.sonatype.com/state-of-the-software-supply-chain

[4] https://www.youtube.com/watch?v=8wIDzfuIGKI

The Legislative Response

Companies and public administrations find themselves at a crossroads: Now more than ever, they need to detect these risky components to prevent potential cyberattacks on their digital infrastructures. Recent international movements include the Cyber Resilience Act (CRA) in Europe, which came into effect on December 10, 2024, and similar movements in the United States. The CRA and similar legislation aim to "protect consumers and entities that purchase software or hardware products with a digital component." And this applies to the digital supply chain.

Digital supply chain risks apply at all levels within Europe, from private companies to public administrations, from municipalities to states and their defense policies. It must be part of states' initiatives to identify, improve, and sustain those software components that are key to their digital infrastructure. And this process must be part of the current contract bidding process for software products and hardware products that contain software.

Open Source Solutions & the Path to Resilience

The digital supply chain must be secure, and those components that are free or that use free dependencies have a clear competitive advantage. This advantage is that their entire development process is carried out transparently, and as such, it can be analyzed and understood. As we embrace free components, we must take into account the following factors:

- Digital sovereignty, or which companies and/or countries are behind development.
- Risk analysis, according to the internal defined standards.
- Development and security practices.

Attacks on the digital supply chain continue to increase every year, affecting all types of services. And they have already had a significant impact on the final cost, reputation, and quality of service. We now have the opportunity to work together at different public and private levels to secure the supply chain and grow our resilience at the European level. This type of collaboration is already happening at organizations like the Sovereign Tech Agency, which invests in different free software projects identified as priorities for the German federal government's digital infrastructure. More efforts like this one must rise to the moment and ensure our digital resilience into the future.

[5] https://digital-strategy.ec.europa.eu/es/policies/cyber-resilience-act
[6] https://www.congress.gov/bill/118th-congress/senate-bill/1526