Zero Trust and Software Supply Chain Security

EU SBOM initiatives

Presented by: Scott CADZOW, ETSI Fellow 2023

August 28th 2023, Goyang, Republic of Korea (remote presentation)

Agenda

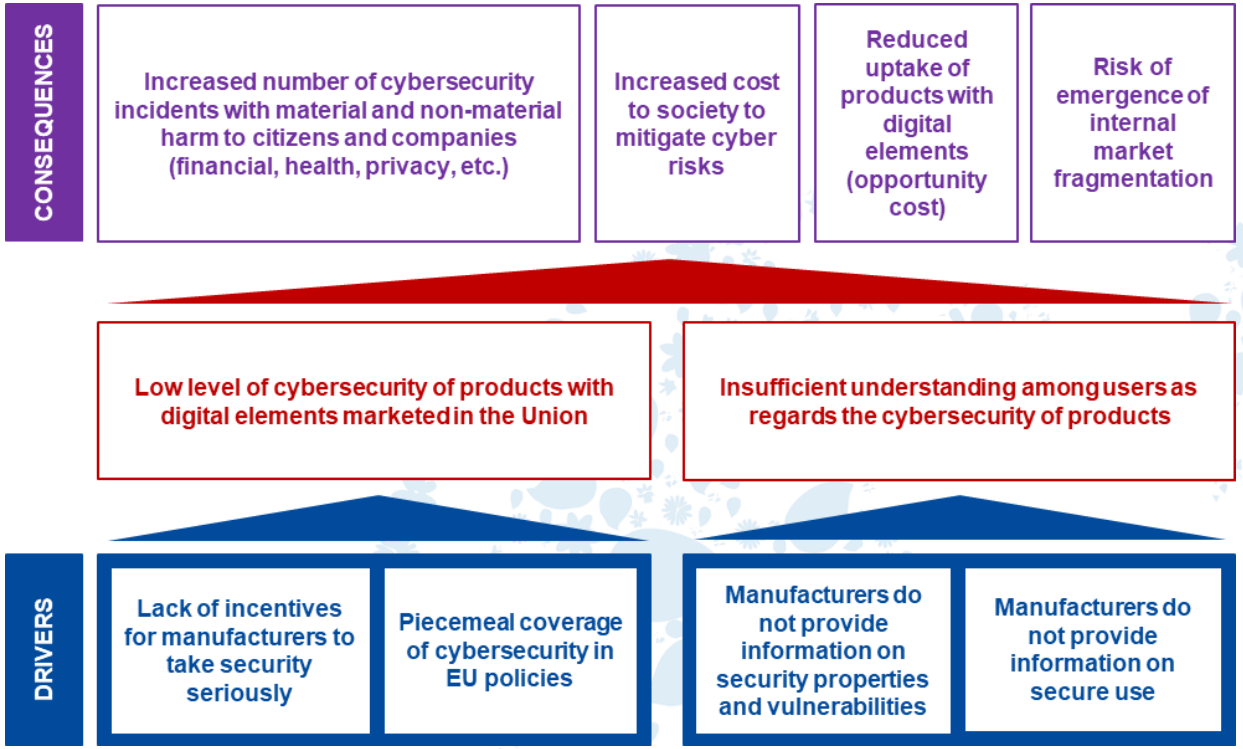
- Overview of EU market evolution
- Primary concerns
- The role of SBOM as mitigation
- Standardisation efforts
- Summary

Overview of EU market evolution

- Telecommunications regulation has evolved from Government controlled and highly regulated (to about 1990), through market controlled with light touch regulation (from about 1990 to now), to a focus on strong market controls with standards conformance explicit in the regulation.
- The role of standards and regulation is now becoming more entwined
    - Cyber Resilience Act, Cyber Security Act, Network and Information Security Directive (v2), Artificial Intelligence Act
    - All of these cite the role of standards and the role of the ESOs in their development
    - EXAMPLE from CRA in Recital 38: In order to facilitate assessment of conformity with the requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements which are in conformity with **harmonised standards**, which translate the essential requirements of this Regulation into detailed technical specifications

Primary concerns (of risk in the software market)

- The picture is taken from the supplementary information for the CRA and exemplifies the issues seen by regulators
- What is the content of software, and how that content is controlled, is one of the drivers that leads to the highlighted consequences



The role of SBOM as mitigation #1

- As cited in the CRA
  - **Recital 15**: The Commission, after consulting the Expert Group and taking account of international standards, is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation by specifying the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I.
  - **Recital 37**: In order to facilitate vulnerability analysis, manufacturers **should** identify and document components contained in the products with digital elements, including by drawing up a **software bill of materials** (SBOMs).
    - A SBOM can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties.
    - Manufacturer should not, however, be obliged to make the software bill of materials public, as this may have unintended consequences on the cybersecurity of their products with digital elements.
  - Annex I, 2(1): Manufacturers of the products with digital elements **shall**: (1) identify and document vulnerabilities and components contained in the product, including by drawing up a **software bill of materials** in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

The role of SBOM as mitigation #2

- Supply chain security and supply chain integrity
  - SBOMs are a representation of the software supply chain for the immediate link back in the chain
  - The collection of all SBOMs represent the full supply chain as an SBOM
  - **ENISA**: Supply chain Integrity has been a recurrent theme of ENISA's reports since 2010 or so.
    - Hardware based supply chains often have alternate suppliers or multiple suppliers for a component
    - The BOM for 2 or more samples of the same item could be significantly different
    - SBOMs or other supply chain transparency tools are identified as the output of a well executed due-diligence exercise

Standardisation efforts (on defining SBOMs)

Many standards are available from many sources

CRA requirements: to use a commonly used and machine-readable format

- The CycloneDX format addresses this in part in both JSON and XML https://cyclonedx.org
- SPDX, available as ISO/IEC 5962 (free download is available)
- CPE (Common Platform Enumeration)

National and international standards efforts:

1) USA (National Telecommunications and Information Administration) → https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf
2) USA (NIST) → Incorporation of CPE into the wider National Vulnerability Database as a semantic identifier
3) ISO → for SPDX as above
4) ETSI → Supply chain and some remarks on SBOMs are found in ETSI TR 103 305 (Security controls)
5) ENISA → Seed for studies into the supply chain incorporating guidance at EU level to ESOs and Parliament

Relationship between SBOMs and Zero Trust

SBOMs are relatively static but have a root in due diligence

- An SBOM identifies where things come from and due diligence actions say why you need those things
- In Zero Trust any “thing” used by, or connected to, an object is treated as untrusted until their integrity, identity and authority are verified - zero trust processes can validate an SBOM (if it’s not on the SBOM it should not pass the ZT checks)

Zero Trust should also enable least persistence and least privilege security objectives

- ZT should assume a framework of due diligence that results in a record of what should be
- The SBOM may act as that record of due diligence for ZT to work

Summary and closing

SBOMs are key elements of the EU's policies for provision of cybersecure products and services to the market

SBOMs are the result of supply chain due diligence

SBOMs are part of the initiative to enforce transparency and explainability/explicability on products containing digital elements

Standardisation of SBOMs is not finalised

1) Formats and syntax/structure to be harmonised (lots of possible standards currently exist)
2) Role of SBOM in wider frameworks such as ZT to be examined
3) Role of SBOMs in determination of geo-source of content may be useful to examine