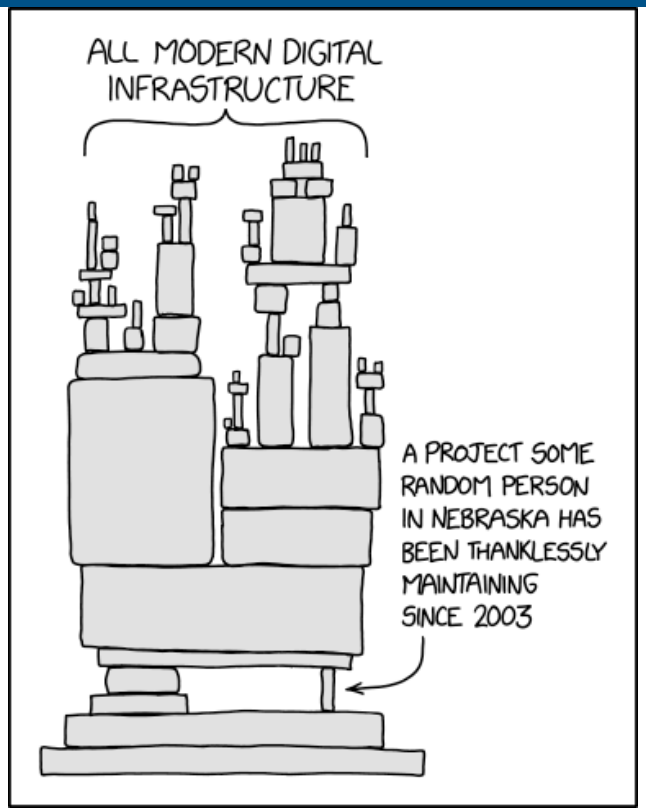
Software Bill of Materials
An Introduction and cross-sector update

Allan Friedman, PhD
CISA Senior Advisor & Strategist

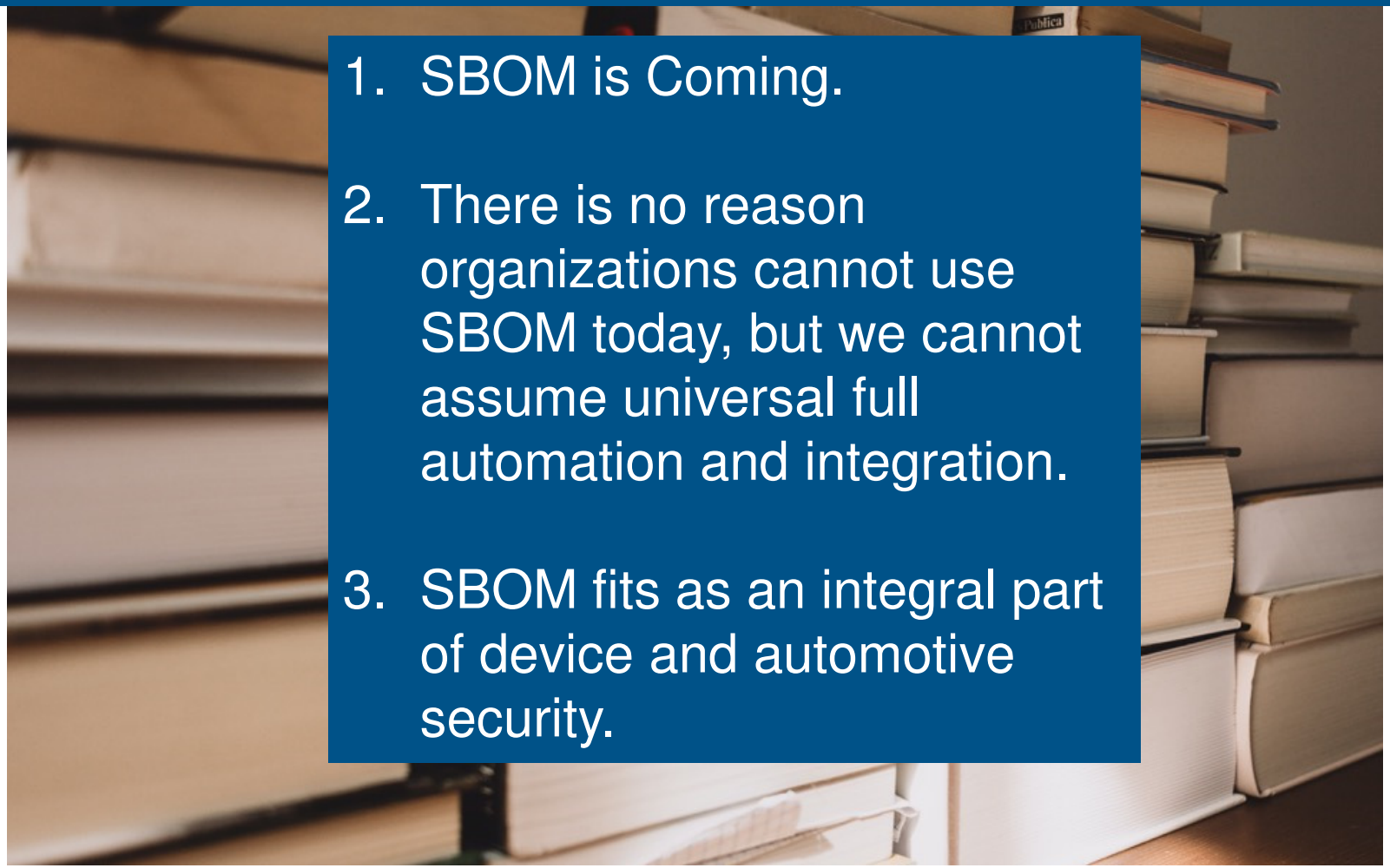
Will this be worth my time?

- The case for transparency
- What is an SBOM?
- Why aren't we doing this today?
- What we've done so far
- Gaps: what we're still working on
- Status of SBOM today



https://xkcd.com/2347/

TL;DR

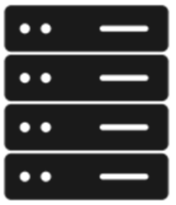


1. SBOM is Coming.
2. There is no reason organizations cannot use SBOM today, but we cannot assume universal full automation and integration.
3. SBOM fits as an integral part of device and automotive security.

Transparency can help markets thrive

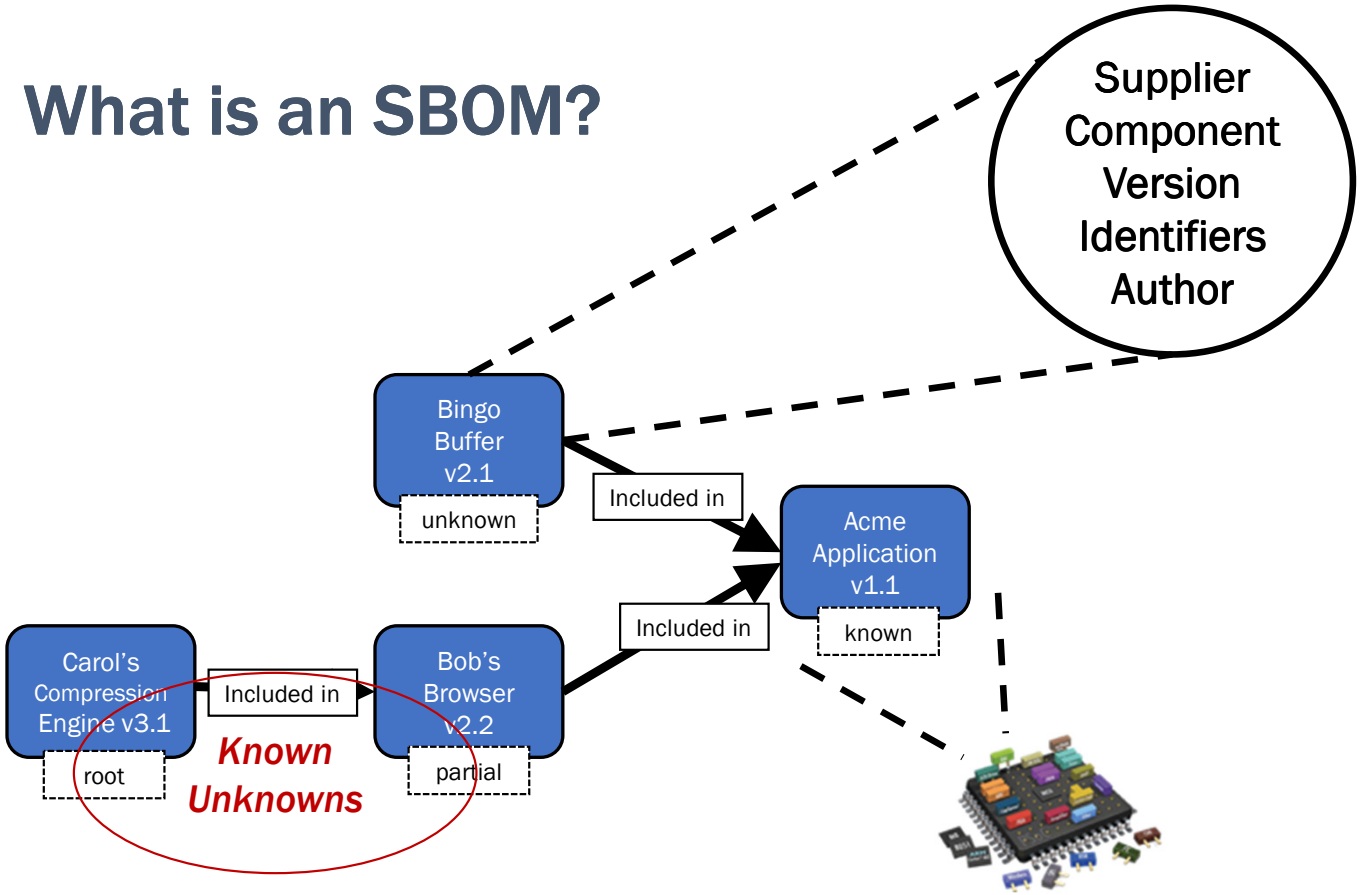
- Food ingredients and food labels
- Safety Data Sheets in the chemical industry
- Hardware Bills of Material (BOM) in industry
- Naming and tracking components can drive innovation (e.g. CVE)

“Know what you have”



LOG4J

What is an SBOM?



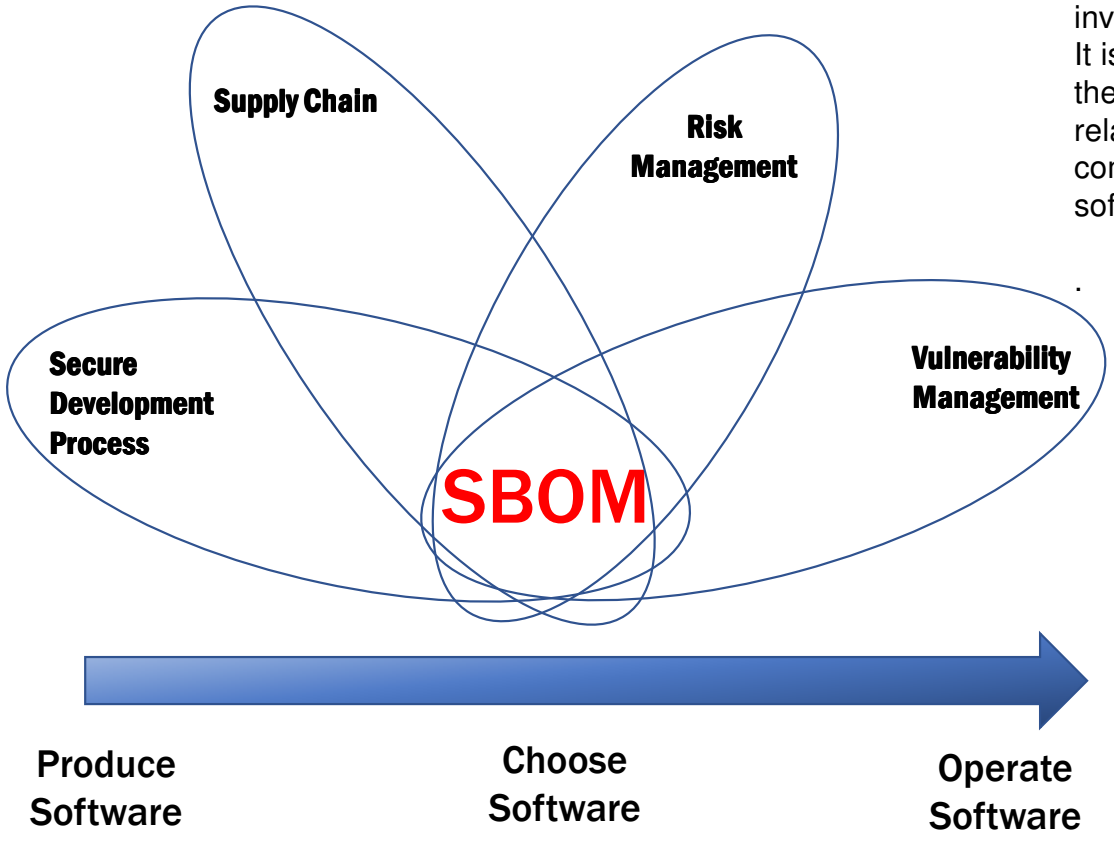
6

Why aren't we doing this today?

- Licensing concerns and open source restrictions
- It's hard: many benefits require machine readability for automation.
- It's complex: involves integrating some technical and operational innovation.
- Need to understand it from a market perspective: supply and demand.

A Software Bill of Materials (SBOM) is effectively a list of ingredients or a nested inventory.
It is “a formal record containing the details and supply chain relationships of various components used in building software"

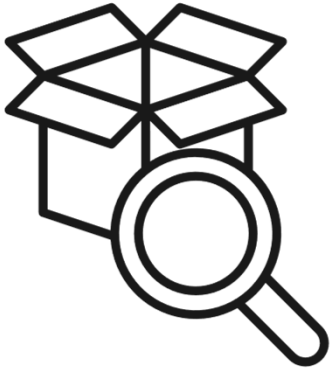
.



Transparency in the lifecycle

source

build



binary analysis

Implementing automation-friendly SBOM

CISA is actively working to help harmonize across these communities

Solution: "Vulnerability Exploitability eXchange" (VEX) implemented in OASIS CSAF


“We like this idea...
We’ll do it when someone makes us.”

Executive Order 14028 (May 12, 2021) “Improving the Nation’s Cybersecurity”

- "The trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is...”
- The EO defines SBOM and identifies the value proposition in 10(j)
- Section 4: Enhancing Software Supply Chain Security.
  - 4(f) –DefineD the “minimum elements” of SBOM
  - 4(e)(vii) –defined guidance on “providing a purchaser a Software Bill of Materials (SBOM) for each product”
  - 4(k) and 4(n) – map guidance into rules

SBOM Minimum Elements

Data Fields	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

Sector-specific implementations

- Healthcare
- Cloud-native technology
- Finance
- Energy
- Automotive

The State of SBOM in 2022

- Tooling is still emerging, especially for consumption.
- No proven, scalable platforms for sharing & exchanging SBOM data.
- Assumptions about seamless interoperability have not been tested.
- Not all vulnerabilities put organizations at risk.

There is no reason organizations cannot use SBOM today, but we cannot assume universal full automation and integration.

SBOM: Part of a complete breakfast

For more information:
www.cisa.gov/SBOM

Questions?
SBOM@cisa.dhs.gov
allan.friedman@cisa.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA