How a Software Bill of Materials is a key factor when securing the supply chain

SWISS CYBER STORM 2021

«Securing the Supply Chain»

Patrick Dwyer

- OWASP CycloneDX Co-Lead
- OSS maintainer
- Multiple SBOM related initiatives
- Software development team lead for a Gov org


@coderpatros


patrick.dwyer@owasp.org

Modern software and embedded devices are assembled using 3rd party components

Benefits include:

- Reduced time to market
- Cost effective
- Quality

ACSC Advisory 2020-008, the “copy-paste” advisory

- Includes CVE-2019-18935, a critical remote code execution vulnerability
- User interface controls for web applications
- CVE and public exploit code available for 6 months prior to “copy-paste” advisory (ಠ_ಠ)

The Impact of Ransomware on Healthcare During COVID-19 and Beyond

Ponemon Institute research report sponsored by Censinet

The Impact of Ransomware on Healthcare During COVID-19 and Beyond

“The purpose of this research is to understand how COVID-19 has impacted how healthcare delivery organizations protect patient care and patient information from increasing virulent cyberattacks, especially ransomware.”

The Impact of Ransomware on Healthcare During COVID-19 and Beyond

“The possible adverse impact on patient care due to third-party risks is the biggest pain point in organizations.”

Figure 13. The consequences of cyberattacks on patient care
More than one response permitted

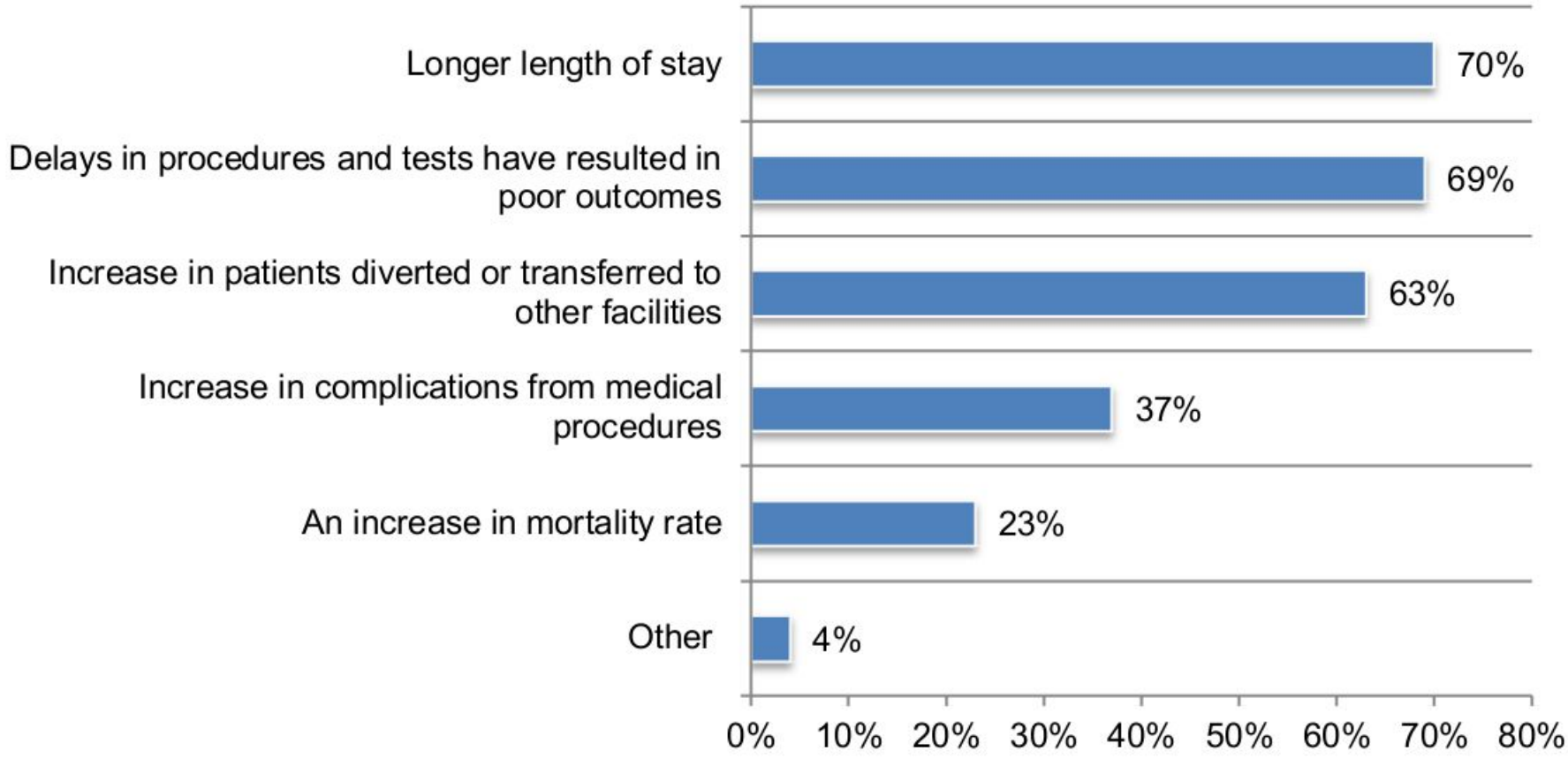
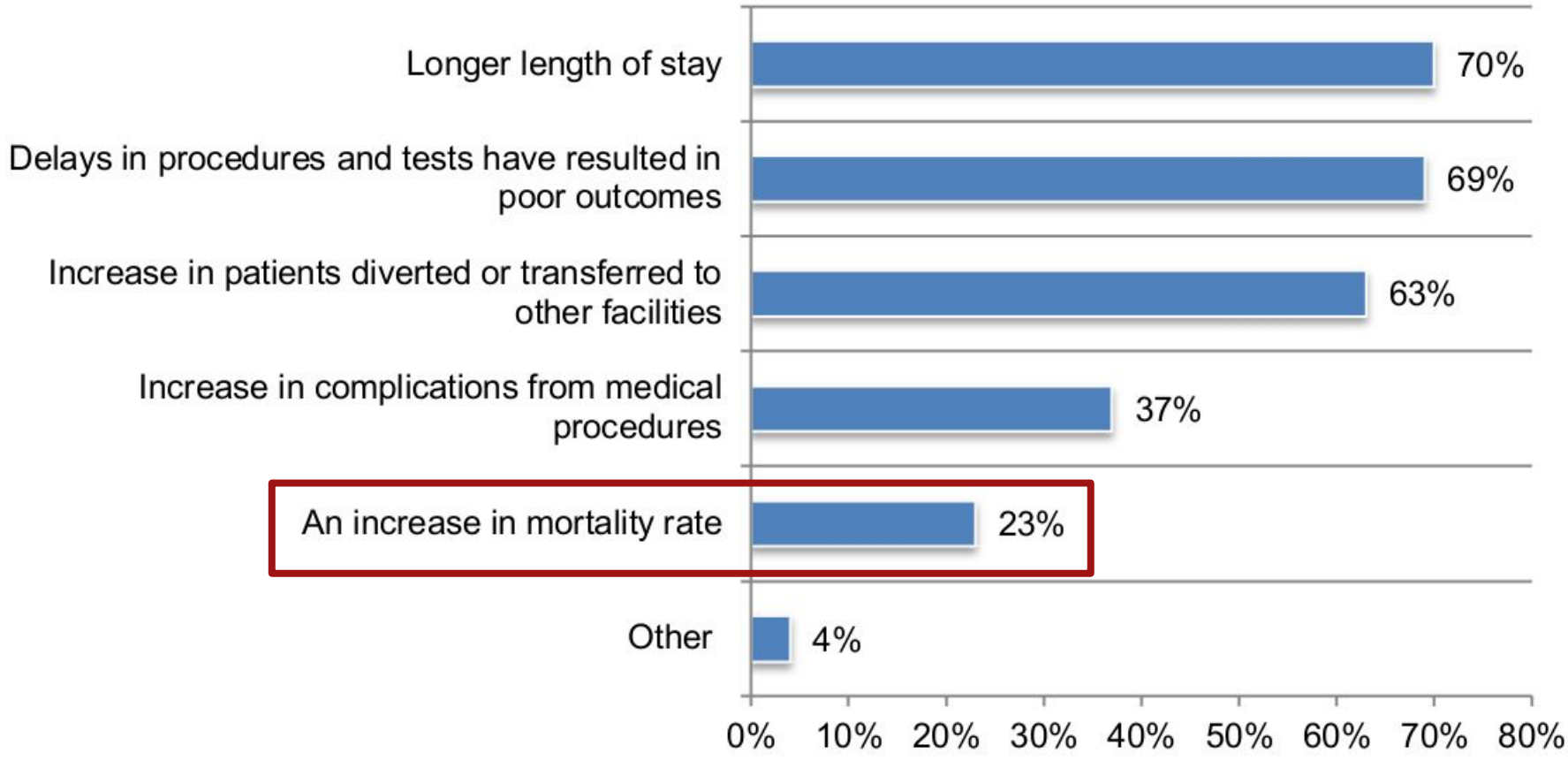


Figure 13. The consequences of cyberattacks on patient care
More than one response permitted



In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

US President Executive Order 14208, Improving the Nation’s Cybersecurity

Are we affected?
Where are we affected?

Food allergies

Food labelling standards

Food labelling standards

- Made in Australia from at least 95% Australian ingredients

Food labelling standards

- Made in Australia from at least 95% Australian ingredients
- Malt extract from barley

Food labelling standards

- Made in Australia from at least 95% Australian ingredients
- Malt extract from barley
- Allergen statement

Food labelling standards

- Made in Australia from at least 95% Australian ingredients
- Malt extract from barley
- Allergen statement
- Enables a risk based approach

Le Parfait

Yeast, water, palm kernel fat, pork liver (12.2%), maltodextrin (from corn starch), potato starch, salt, sunflower oil, modified maize starch, black trumpet mushrooms, spice and herb extract.

(Photo credit: Heddi Nieuwsma, Cuisine Helvetica https://cuisinehelvetica.com/)

Le Parfait

- Acquired by Nestlé in 1971

(Photo credit: Heddi Nieuwsma, Cuisine Helvetica https://cuisinehelvetica.com/)

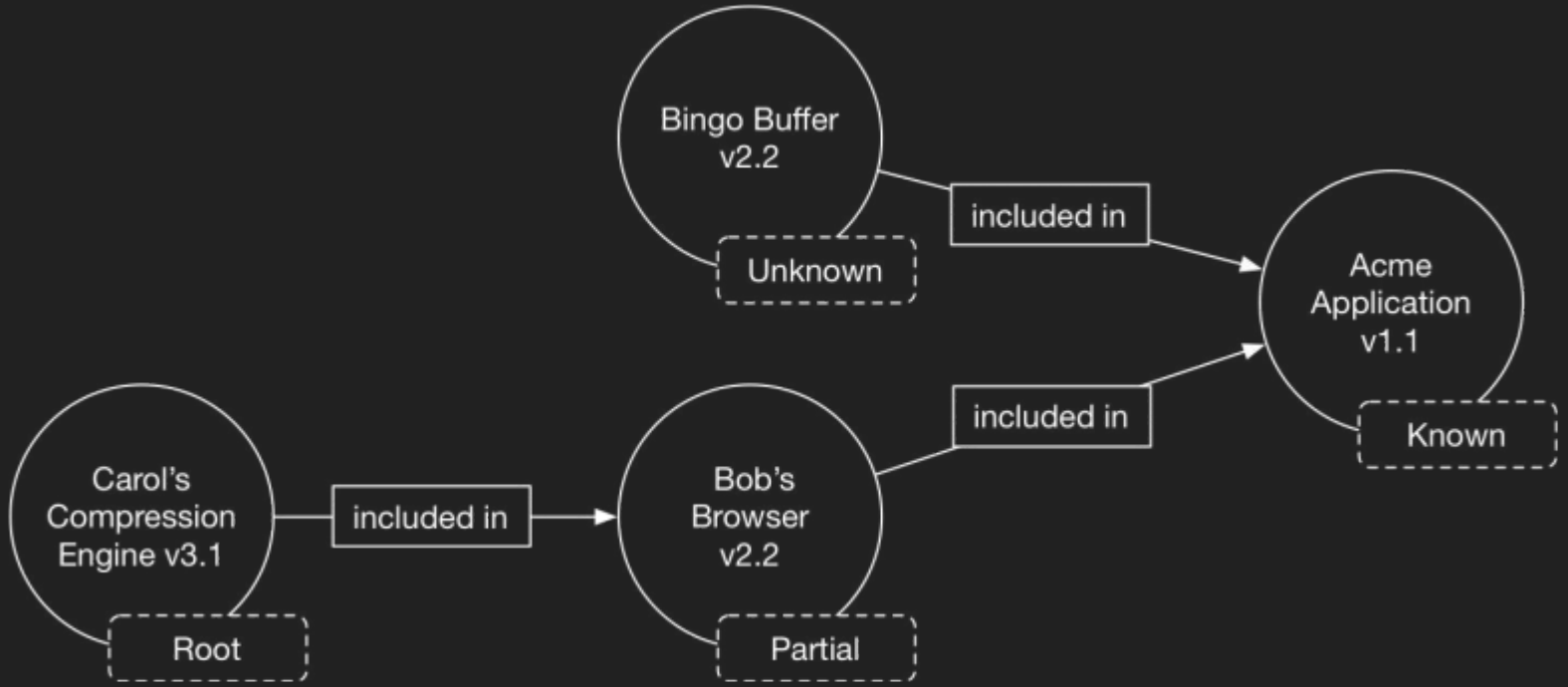
Le Parfait

- Acquired by Nestlé in 1971
- Truffles were one of the ingredients up until the 1990’s, replaced with black trumpet mushrooms

(Photo credit: Heddi Nieuwsma, Cuisine Helvetica https://cuisinehelvetica.com/)

Software Bill of Materials

(Photo credit: Zdeněk Patera, Auta5P https://auta5p.eu/)



(Credit: NTIA SBOM at a Glance)

Software Bill of Materials - key information

- Component name
- Version
- Author
- Supplier
- Unique identifier
- Licence
- Hash

SBOM Formats

SPDX is an open standard for communicating software bill of material information (including components, licenses, copyrights, and security references). The SPDX specification is developed by the SPDX workgroup, which is hosted by The Linux Foundation. The grass-roots effort includes representatives from more than 20 organizations—software, systems and tool vendors, foundations and systems integrators. It is specified in ISO/IEC 5962:2021.

OWASP CycloneDX is a software bill of materials (SBOM) standard, purpose-built for software security contexts and supply chain component analysis. The specification is maintained by the CycloneDX Core working group.

SWID tags record unique information about an installed software application, including its name, edition, version, whether it is part of a bundle and more. SWID tags support software inventory and asset management initiatives. The structure of SWID tags is specified in international standard ISO/IEC 19770-2:2015.

SBOM use cases

SBOM use cases

- Procurement

SBOM use cases

- Procurement
- Product lifecycle

SBOM use cases

- Procurement
- Product lifecycle
- Software portfolios

SBOM use cases

- Procurement
- Product lifecycle
- Software portfolios
- Impact analysis

SBOM use cases

- Procurement
- Product lifecycle
- Software portfolios
- Impact analysis
- Pedigree and provenance

SBOM use cases

- Procurement
- Product lifecycle
- Software portfolios
- Impact analysis
- Pedigree and provenance
- Licence compliance

SBOM use cases

- Procurement
- Product lifecycle
- Software portfolios
- Impact analysis
- Pedigree and provenance
- Licence compliance
- Integrity

SBOM use cases

- Procurement
- Product lifecycle
- Software portfolios
- Impact analysis
- Pedigree and provenance
- Licence compliance
- Integrity
- Services and endpoints

SBOM use cases

- Procurement
- Product lifecycle
- Software portfolios
- Impact analysis
- Pedigree and provenance
- Licence compliance
- Integrity
- Services and endpoints
- Component risk

Getting started - consumers

- Procurement
- Vulnerability advisory SLA

Getting started - producers

- Be open and transparent with yourself
- Focus on high value/risk products
- Vulnerable dependencies
- Outdated components
- Open source licence compliance

"You can't defend what you don't know about."

Dr Allan Friedman, US Cybersecurity and Infrastructure Security Agency

More Information

https://www.ntia.gov/sbom
https://cyclonedx.org/
https://spdx.dev/
https://csrc.nist.gov/projects/Software-Identification-SWID