



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SUPPLY CHAINS UNDER THREAT

CYBER SECURITY COALITION - CYBER EXPERIENCE SHARING
DAY

Dr. Evangelos Ouzounis, Head of Policy Development and Implementation Unit, ENISA

8 | 10 | 2024

AGENDA

- Key trends – supply chain risks
- Current practices by entities in the EU
- Good practices guide
- Conclusions

KEY TRENDS – ENISA THREAT LANDSCAPE 2024

Supply chain security is a growing concern

- 2021: 66% of supply chain attacks focus on the supplier's code
- 2021: Advanced persistent threat actors demonstrate a continuous interest and increased capability in supply chain attacks
- 2023: continued activity by threat actors, making use of software update mechanisms to deliver malware to victims or to compromise the open-source software supply chain
- 2023: most targeted are identity providers, IT suppliers and managed service providers
- 2023: Threat actors focus on employees as an entry point for organisations, especially targeting those with privileged access by using social engineering techniques
- 2024: Supply chain attacks are often linked to geopolitics, as threat actor aims to disrupt flows linked to ongoing conflicts (aid, military)
- 2024: out of the observed events that ENISA collected, supplier sectors were targeted, e.g. Digital infrastructure (8%), manufacturing (6%), business services (8%), energy (3%) and ICT service management (3%).





RECENT INCIDENTS

- Okta Hack (January 2022): The Lapsus\$ group gained access to Okta's network via a third-party subprocessor, Sitel. This allowed them to view customer information and perform administrative actions, impacting approximately several customers.
- GitHub OAuth Tokens Attack (April 2022): Attackers stole OAuth tokens issued to third-party integrators Heroku and Travis-CI, affecting several GitHub customers.
- MOVEit Supply Chain Attack (June 2023): Attackers exploited vulnerabilities in the MOVEit file transfer software, impacting numerous customers relying on MOVEit for secure data transfers.
- JetBrains Supply Chain Attack (September/October 2023): Attackers targeted JetBrains, a software development company, and compromised their software distribution channels. This allowed the attackers to inject malicious code into JetBrains products, affecting many users.

What about system failures or user errors at the supplier side?

CrowdStrike (July 2024) released an update to its Falcon endpoint detection and response agent. This update contained flaws that caused widespread issues, including the infamous “blue screen of death” on millions of Microsoft Windows machines.

KEY TRENDS FORESIGHT CYBERSECURITY THREATS FOR 2030 - UPDATE 2024

1. Supply Chain Compromise of Software Dependencies
4. Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem
7. Cross-border ICT Service Providers as a Single Point of Failure



ARE WE PREPARED?

SURVEY conducted in 2022

- Executed by ENISA, April to June 2022
- All 27 EU MS, minimum 40 OES and DSPs per MS

INCIDENTS

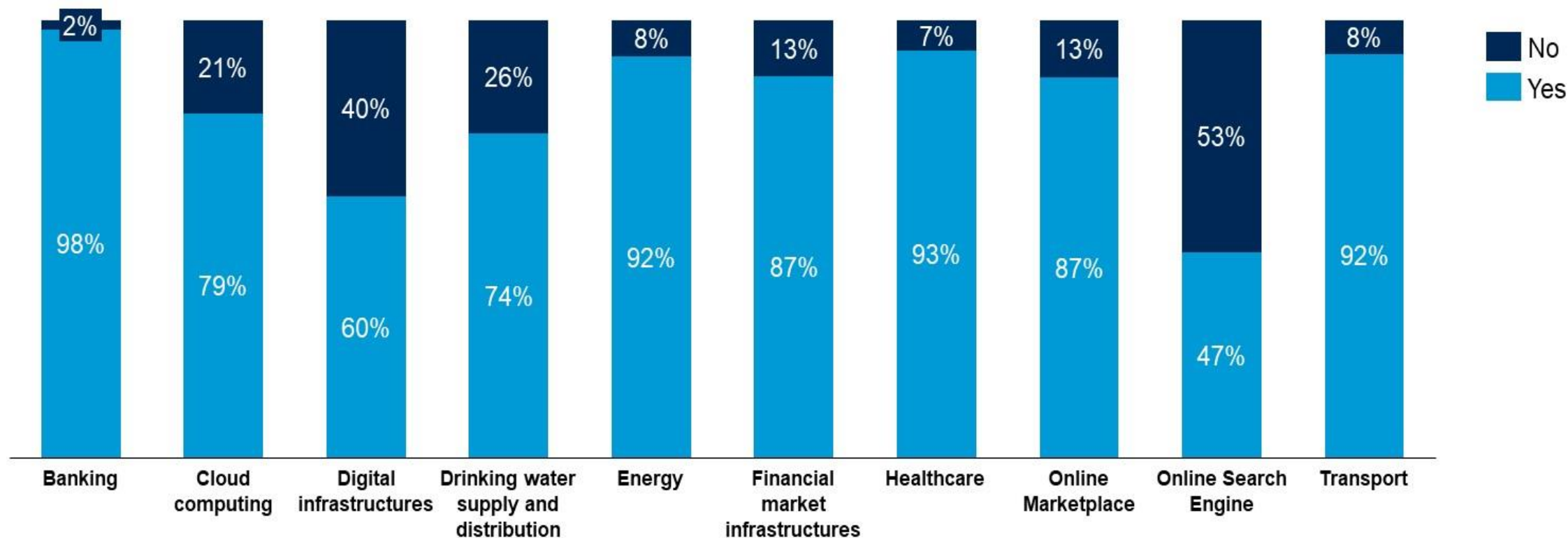
- ENISA's annual threat landscapes
- ENISA's situational awareness sources
- NIS Cooperation Group Annual report

REGULATORY FRAMEWORK & STANDARDS

Desktop research - more than 17 documents

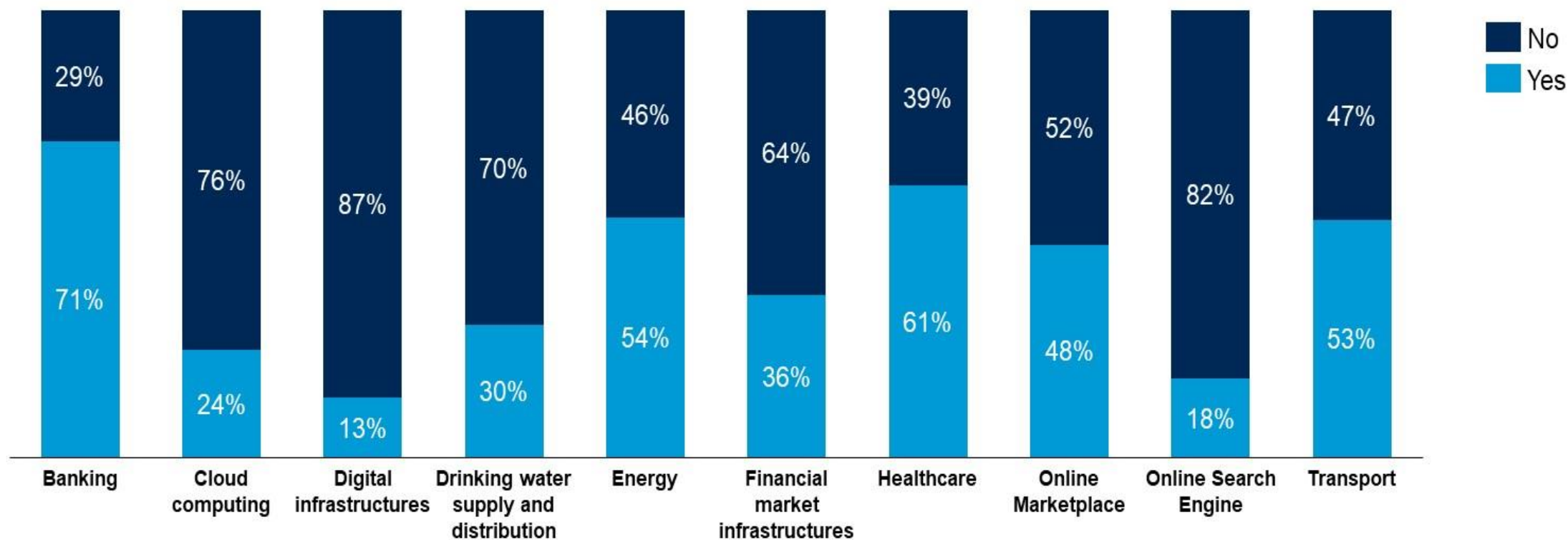


SUPPLY CHAIN RISK MANAGEMENT POLICIES PER SECTOR



Operators do not allocate the necessary resources for supply chain risk management cybersecurity. The majority of investments is without clear governance structures. The percentage of OESs and DSPs with third-party risk management policies increases from 36% to 87% when management signs-off on cyber risk management measures. However, large enterprises are more likely to have a policy (85%) compared to SMEs (53%). The approach is affected by the maturity of the sector, size of the entity and the commitment of top management.

DEDICATED SUPPLY CHAIN CYBERSECURITY BUDGET



Only 47% of the OESs and DSPs had earmarked a dedicated budget for third-party risk management. Only 24% of the OESs and DSPs had dedicated employees for third-party risk management.

OTHER FINDINGS

- When assessing their third-party risks, 61% of the OESs and DSPs take into account **whether a supplier is certified**, use **security risk rating services** (43%) and perform **due diligence or risk assessments** (37%). Moreover, the entities take into account the **type of product or service** (59%), the **volume of spending with the supplier** (47%) and **whether or not the supplier is subject to the NIS1 Directive** (42%).
- **48%** of the OESs and DSPs had implemented a **risk-based vulnerability management process**, with 26% covering only internet-facing assets and 22% only covering critical assets. Whereas 37% of the OESs and DSPs had partially implemented a risk-based vulnerability management process, it may be noted that only **15% did not have such processes at all**.
- The majority of OESs and DSPs (52%) had a rigid patching policy, in which only 20% or less of their assets are not covered. On the other hand, **13.5% of the surveyed OESs and DSPs had no visibility over the patching of 40% or more of their information assets**.
- **46%** of OESs and DSPs **patch critical vulnerabilities in less than a month**. Furthermore, an equal percentage of the organisations surveyed indicated that they patch critical vulnerabilities within six months or less. Only 8% of the organisations surveyed indicated that they exceed this time and take longer than six months to patch critical vulnerabilities in their systems.



REGULATORY INITIATIVES

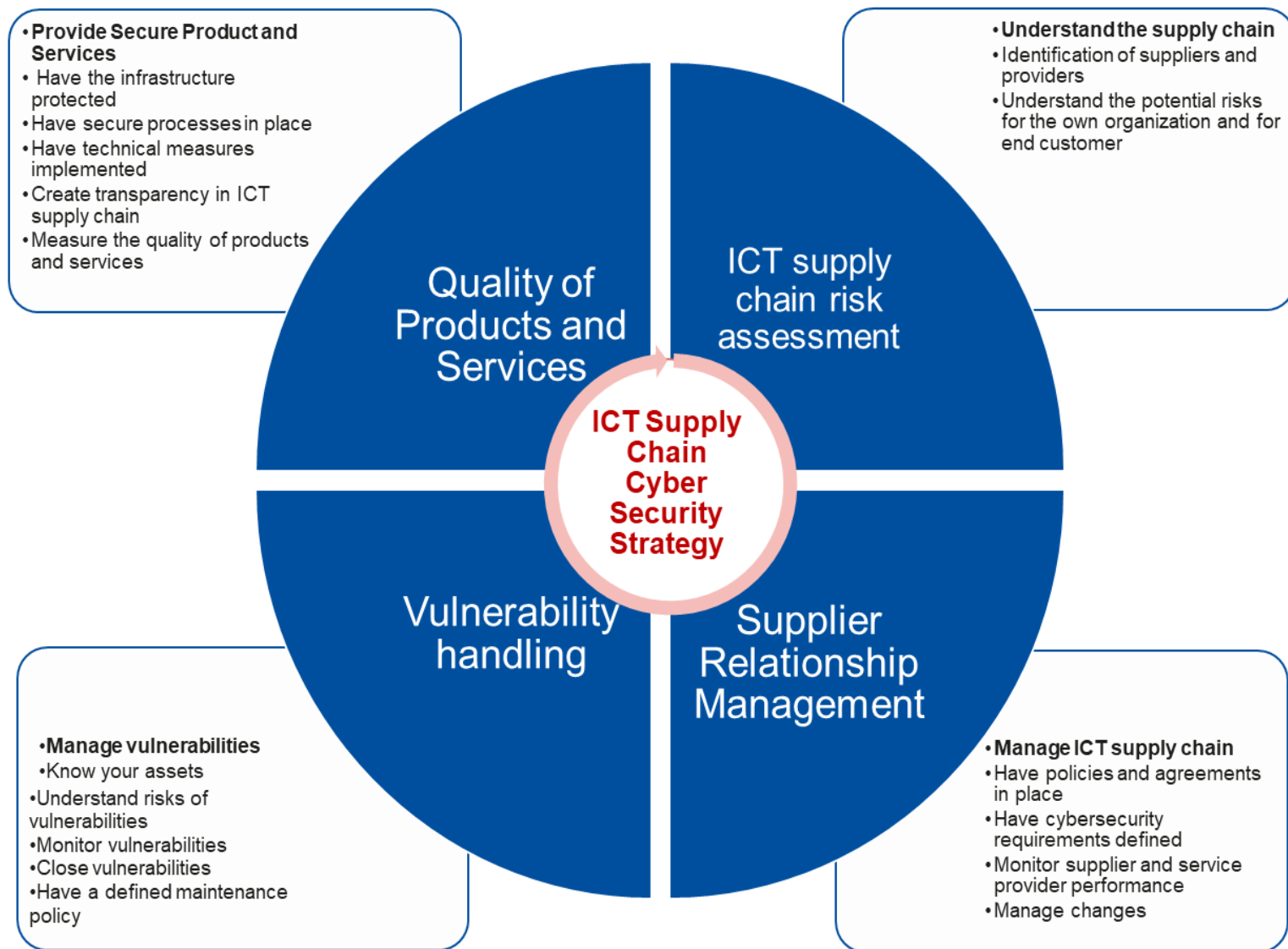
- **Cyber Security Act (2019): certification of products and services**
- **NIS2:**
 - Supply chain cyber security is part of the national cyber security strategies
 - Entities shall take appropriate measures for securing their supply chains
 - National coordinated risk assessments (for the NCAs) – ICT supply chain toolbox been prepared
- **Cyber Resilience Act:**
 - Harmonised rules when bringing to market products or software with a digital component;
 - A framework of cybersecurity requirements governing the planning, design, development and maintenance of such products;
 - An obligation to provide duty of care for the entire lifecycle of such products.



NIS2 AND SUPPLY CHAIN

- **Operators shall take**

- **appropriate** and **proportionate** technical, operational and organisational measures
 - measures which are based on an **all-hazards** approach
- into account **relationships** with their direct suppliers or service providers
- into account the **vulnerabilities** specific to each direct supplier and service provider
- into account the **quality of products** and cybersecurity practices of their suppliers and service providers



SUPPLY CHAIN RISK MANAGEMENT CYCLE

IN LINE WITH NIS2

BASED ON
STANDARDS AND
GOOD PRACTICE
DOCUMENTS

<https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity>



CONCLUSIONS

- Supply Chain Compromise of Software Dependencies is considered the top emerging threat among the Cybersecurity threats for 2030.
- Supply chain attacks are here to stay and are growing further. Threat groups demonstrate a continuous interest and increased capability in supply chain attacks.
- Strong security protection is no longer enough for organisations when attackers have already shifted their attention to suppliers.
- Operators do not allocate the necessary resources for supply chain cyber risk management.
- The need to act is clear: good practices and coordinated actions are important to reach a common high level of cybersecurity.
- Supply chain cyber security provisions become integral part of the majority of (sectorial) cybersecurity initiatives.

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece



Supply Chains Under Threat



info@enisa.europa.eu



www.enisa.europa.eu

