
# SUPPLY CHAIN ATTACKS

Co-funded by the European Union

***ESCAPE.*** *Preparing healthcare professionals for cyberattacks*
*Project No.2023-1-ES01-KA220-VET-000151536*

# Partners


ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS Weser

**ESCAPE. Preparing healthcare professionals for cyberattacks**
**Project No.2023-1-ES01-KA220-VET-000151536**

Co-funded by
the European Union

*This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*

# Table of Contents


1. Definition 1
2. General Importance 1
3. Importance in Health and Care, and Impact on Quality of Care 1
4. What Can I Do as a Healthcare Professional? 2
5. More Information
    1. Learning Materials 2
    2. Relevant Videos 2
    3. Relevant Links 3
6. Bibliography 3



Co-funded by the European Union

# FACTSHEET – SUPPLY CHAIN ATTACKS

## 1. Definition

It occurs when a malicious actor targets an organisation by compromising less secure elements in its supply chain rather than the main organisation directly, such as third-party vendors or service providers, to gain access to the main target1.

This makes it difficult to find and affects a large number of people, as a single breach can affect multiple organisations downstream.

## 2. General importance

Due to organisations' heavy reliance on third-party networks, supply chain attacks are becoming a more serious worldwide threat. Because of this connection, attackers can go after a smaller, less secure supplier instead of trying to break into a system that is well protected2.

All of the above makes it difficult to detect this type of breach. Often, it appears as a legitimate update or system operation. It just takes one compromised provider to expose thousands of clients.

Also, supply chain attacks are strategically appealing to both state-sponsored groups and cybercriminals because they have the biggest effect and reach. As more people use cloud services and services from other companies, the chances and effects of these kinds of attacks are expected to get much worse3.

## 3. Importance in health and care, and impact in quality of care

A supply chain attack in the healthcare sector not only leads to financial or reputational loss but also impacts patient safety and quality of care4. As hospitals rely on third parties (e.g., electronic health records, diagnostic and imaging systems, cloud services, etc.), a breach could mean total access to sensitive patient data, causing psychological distress or financial fraud against patients5.

This situation has a significant impact on quality of care. Sources describe how ransomware delivered through a supply chain compromise could delay surgeries, postpone lab results, etc., which may increase morbidity and mortality rates in emergencies.

## 4. What can I do as a healthcare professional?

- Report any unusual system behaviour.
- Be careful with emails, portals, or apps from third-party providers.
- Follow organisational protocols and always adhere to security restrictions.
- Take part in cyber training and keep up with how supply chain risks manifest in your daily work.

## 5. More information

### 5.1 Learning Materials

- Web seminars about key aspects of cibersecurity (JGT-3)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- An article on security strategies applicable to electronic patient records (IST-37)
- An infographic on security and cybersecurity devices used in different healthcare settings. (IST-38)
- Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview (PRAMMER-33)
- A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia (PRAMMER-34)

### 5.2 Relevant Videos

This video describes what malicious supply chain attacks are, how they are identified and dealt with, and how industry organisations can prevent them.

| **What is Supply Chain Attack \| Supply Chain Attacks in Cyber Security \| Intellipaat** |
|---|
| https://www.youtube.com/live/LIkxOiNOkec?si=W-h6-lM893uKdTnt |

This video discusses how weaknesses in third-party software and hardware providers can make healthcare systems more vulnerable to cyberattacks, which can put patient safety and operational resilience at risk.

| **How Supply Chain Makes Healthcare Vulnerable to Cyber Attacks** |
|---|
| https://youtu.be/IFBBxNiKysY?si=0UhDHhqvG2LC8DTh |

This short video called "2 Minute Drill" talks about recent supply chain breaches and how they put patients' safety at risk in healthcare systems.

| **2 Minute Drill: Supply Chain Breaches and Patient Safety Risks with Drex DeFord** |
|---|
| https://youtu.be/mi9t_AhLcIQ?si=kheM-OWdkFZG1hyD |

### 5. 3 Relevant Links

This article describes a case where Shields Health Care Group, Eye Care Leaders, and MCG Health were involved in supply chain breaches that collectively impacted over 4.3 million individuals. Shields alone affected around 2 million patients. These incidents show how a single compromised vendor can jeopardise multiple healthcare providers' patient data. https://planet9security.com/supply-chain-attacks-in-healthcare-the-case-of-shields-eye-care-leaders-and-mcg-health/?

A Spanish major pharmaceutical distributor, Alliance Healthcare, suffered a cyberattack that shut down its website, billing systems, and order processing. Alternative supply routes limited the impact on patients, but the disruption highlighted the risks associated with medicine distribution channels. https://www.scworld.com/news/cyberattack-hits-spanish-pharmaceutical-company-alliance-healthcare?

## 6. Bibliography


ENISA threat landscape: Health Sector - CYBIL portal. (2023, 5 julio). Cybil Portal. https://cybilportal.org/publications/enisa-threat-landscape-health-sector/

Organization, W. I. P. (2022). Global Innovation Index 2022: What is the Future of Innovation-driven Growth? WIPO. https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-en-main-report-global-innovation-index-2022-15th-edition.pdf

Lella, I., Theocharidou, M., Tsekmezoglou, E., Malatras, A., & García, S. (2021). ENISA Threat Landscape for Supply Chain Attacks. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf

BobSulli. (2024, 17 octubre). The 2024 Study on Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care | Ponemon-Sullivan Privacy Report. https://ponemonsullivanreport.com/2024/10/the-2024-study-on-cyber-insecurity-in-healthcare-the-cost-and-impact-on-patient-safety-and-care/

European Data Protection Board (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf


**ESCAPE. Preparing healthcare professionals for cyberattacks**
**Project No.2023-1-ES01-KA220-VET-000151536**

**Co-funded by the European Union**







This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.