A Trend Micro Research Report

Healthcare Supply Chain Attacks

Discover where and how to protect your healthcare organisation against the latest threats.

INTRODUCTION

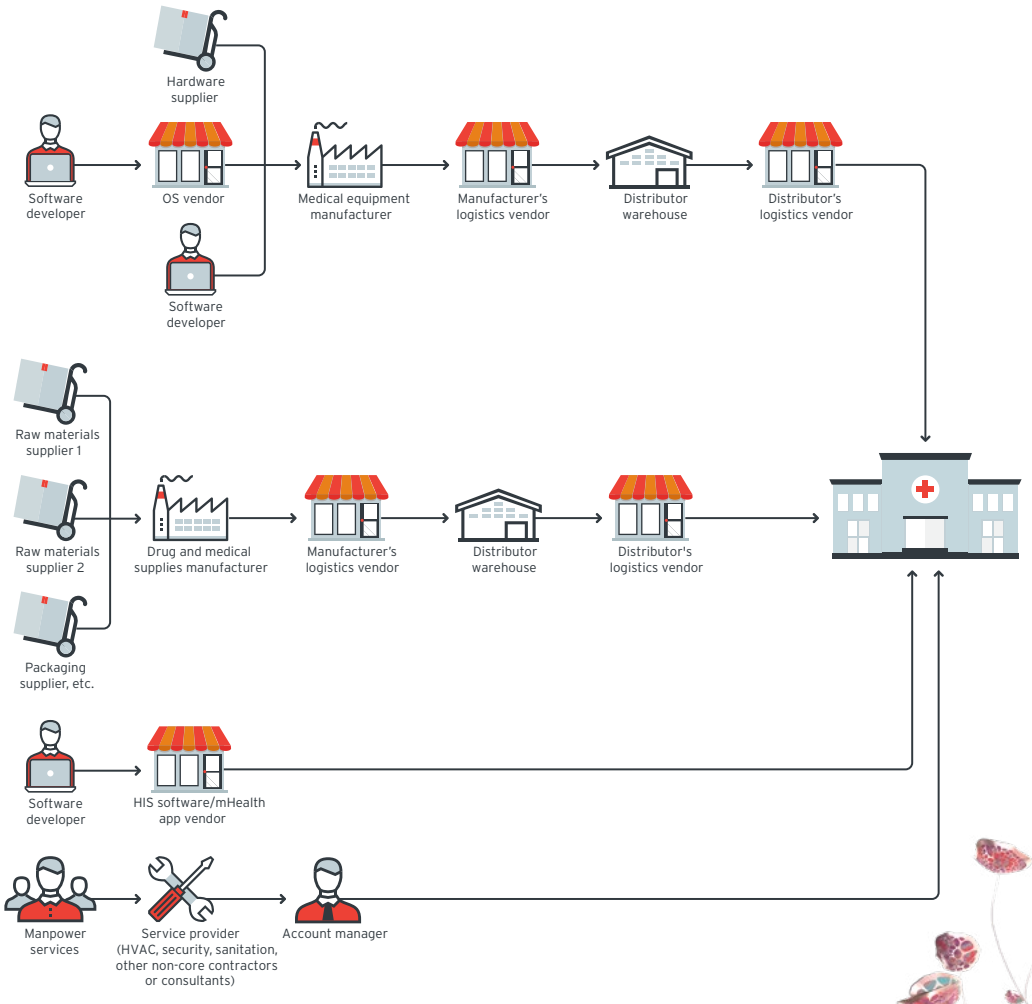
Supply chain volatility has dominated headlines in recent years – and rising cyber-attacks have played a leading role in the disruption. With long and complex supply chains, healthcare organisations are particularly vulnerable. But when you know what the main threats are, and where they frequently occur, it's far easier to protect your organisation, your employees and ultimately, your patients.

Read on to learn more, including:

- Where threats arise in hospital supply chains
- The most common types of attacks
- Recommendations to strengthen your own supply chain

WHERE DO THREATS ARISE IN HOSPITAL SUPPLY CHAINS?

In practice, there are numerous potential entry points that threat actors can use to compromise the hospital supply chain. Below, we show how any products, medicines or supplies you've purchased may come into contact with multiple individuals and companies – and how a lack of knowledge over vetting procedures or security protocols can introduce risk into your organisation.



Risks from manufacturing and shipping

- **Manufacturer:** Without complete visibility, it's impossible to know if the products you've ordered have been tampered with at the manufacturing level.
- **Distribution centre:** Arriving at the distribution centre, the potential for a security breach continues as your products are handled by different onsite personnel.
- **Shipping and transportation:** There's yet another opportunity for tampering as your products are passed to a logistics vendor.
- **Supplier network:** Before reaching your hospital, your products might be stored and repacked by multiple suppliers with different (or no) standardised security practices.

Risk from your own people

- **Current employees and contractors:** Threats can be introduced into your network by your own employees or contractor staff, making strict background checks essential.
- **Previous employees:** Unless access has been terminated completely, it's hard to know if former employees are abusing access privileges, or even exploiting authentication weaknesses.

Risks from software development

- **Software development:** Lack of security safeguards at the app or software level can lead to the discovery or exploitation of vulnerabilities further down the road.
- **Outdated and unpatched firmware:** Medical devices/equipment feature embedded firmware that needs periodically updating to prevent malware infection. Threat actors can leverage these open security holes to compromise the hardware or access the network.

WHAT TYPES OF ATTACKS ARE MOST COMMON IN HOSPITAL SUPPLY CHAINS?

We have identified the seven major supply chain threat vectors that perpetrators may use in the healthcare industry:

1. Firmware attacks on devices

Perpetrators can access and modify the firmware source code of a medical device to add backdoors, which can then be pushed out via existing auto-update mechanisms. Firmware updates are conducted separately from the medical device's software, which requires patients to visit their doctor or healthcare facility to implement the changes.

Hacking the human heart

In 2015, Dr. Marie Moe (a senior security researcher and engineer) wanted to know if the pacemaker in her own heart could be hacked. Her team recently shared their wider research on this topic, which showed that commercial pacemakers have a range of vulnerabilities that could be potentially exploited.

2. Compromises to m-Health mobile applications

m-Health mobile apps can be compromised to change functionality, deliver fatal-level dosage, expose personal health data, and more. They're also at risk from third-party companies that supply services for hosting, server, and cloud solutions. In addition, m-Health apps are not required to report any breaches to the HHS public site, which makes tracking any compromise harder to address.

Mobile health apps are open to attack

In a 2020 global assessment of popular m-Health apps, 91% of the apps tested were found to have weak encryption – and 71% contained at least one fatal security flaw. All of which elevates the risk of sensitive data being exploited.

3. Compromising source code during manufacturing

Perpetrators can access and modify the source code of a vendor by installing a backdoor or rooting the device. Because hospitals tend not to test device security before installing it on their networks, this can cause malware infections, exfiltration of data, and inadvertent sharing of data with third-party vendors or advertisers.

Infecting devices at the operating level

In an especially high-profile example, 17,000 Chinese Android tablets sold on Amazon and other retailers were found to be infected with the Cloudsota Trojan at the operating level, meaning it couldn't be removed. The infected tablets were traced to over 150 countries, making this a truly global incident.

4. Insider threats from hospital and vendor staff

Insider threats can be intentional (such as data theft) or unintentional (such as accidental disclosure or disposal of records). In both cases, they can come from a hospital's current or past employees, as well as hired contractors and seasonal staff. To minimise risk, it's imperative that thorough background checks are performed prior to onboarding, and at regular intervals thereafter.

Insider threats often come from human error

Insider threats aren't always the result of malicious intent. In 2020, NHS documents relating to a Covid-19 contact-tracing app were inadvertently left on a Google Drive that were visible to anyone with a link. The documents included notes on "measuring success" of the app and government projections on the percentage of people likely to download the app.

5. Compromises to websites, EHR, and internal hospital software

Perpetrators can attempt to compromise hospital websites, EHR software, and internal portals used by hospital staff and vendors. Web-based EHR systems suffer from many common vulnerabilities that might give attackers access to backend systems and data.

When electronic health records are left out in the open

In 2021, the records of over two million patients were accessed by a group of hackers who infiltrated the database of Eye Care Leaders – an electronic medical record platform based in the US. To date, there is no evidence to suggest any records have been used by unauthorised individuals, but investigators say the possibility cannot be definitively ruled out.

6. Phishing from trusted email account

Phishing emails involve a perpetrator gaining control of vendor credentials and sending emails that appear legitimate. These forms of deception are getting harder to detect as scammers refine the authenticity of their messages.

Email phishing attack targets NHS workers

Over 1,000 phishing emails were sent from compromised NHS inboxes over a six-month period between 2020-2021. The emails originated from the accounts of 139 NHS employees, the majority of which involved notifications for fake new documents that had links to credential harvesting sites.

7. Third-party vendors

Third-party vendors have credentials that include logins, passwords, and badge access, all of which can be compromised. In addition, they sometimes store physical records, hospital office equipment, and medical devices. Healthcare IT teams need to be vigilant to supply chain risks posed by third-party connections (both physical and digital). A risk-based vendor management program (under a comprehensive enterprise risk management/ governance framework) can assist in minimising these threats.

Hacking patient data in the cloud

A data breach affecting two million patients was reported in March 2022 by Shields Health Care Group. Shields provides a range of medical services for 56 healthcare facilities across New England. The hacker is reported to have accessed a number of Shield's systems for three weeks, stealing a range of patient data, including names, Social Security numbers and billing details.

COMBAT SUPPLY CHAIN RISKS WITH INDUSTRY-LEADING SECURITY.

Risks within healthcare supply chains are often overlooked, but the threats are very real. From the vendors with access to your internal networks, to the suppliers and software developers that provide you with critical medicines and devices. The multiple moving parts that help you deliver life-preserving care can also endanger those very services.

Experience the power of Trend Micro Vision One™

Take a test drive of our purpose-built threat operations platform designed for SOC and security analysts.

Follow these instructions to start a Trend Micro Vision One™ trial.