



CHdN

CENTRE HOSPITALIER DU NORD

From Synnovis to Change Healthcare: Why third-party cyber risk is now a patient-safety issue under NIS2

A practical roadmap from headline horror stories to compliance-plus resilience

4th NISDUC Conference: building a strong and trusted cybersecurity & NIS2 community towards informed governance



**814 surgeries cancelled–
London, June 2024**

About me



Florent Lesueur



15 years in cybersecurity



CISO at CHdN, Luxembourg



lu.linkedin.com/in/florent-lesueur-7381a21a

Case 1: Synnovis, London, 3 Jun 2024



Russian Qilin ransomware
paralysed Synnovis pathology
IT



10,152 appointments and
1,710 surgeries postponed; 2
patients left with permanent
harm



Blood-matching offline;
hospitals used O-type stock,
triggering nationwide
shortage



Hackers leaked 300 M patient
records after unpaid \$50 M
ransom demand

One lab outage cancelled surgeries and drained the UK's blood stock—proof that supplier cyber risk hits patient safety first.

Case 2: Change Healthcare — 21 February 2024 (USA)



Old RDP server, no MFA



\$1.6 B total cost; \$22 M
ransom to BlackCat



Reimbursement and discharge
delay



40 % of US claims — 15 B
claims/year

One upstream breach froze care funding and exposed a third of America—exactly the supply-chain risk NIS 2 aims to prevent.

Major third-party cyber risks

- Exposed vendor portals
- Compromised software update
- Cloud/SaaS outage
- Partner hacked
- Data leakage



Same entry points, same outcome: disrupted care and regulator scrutiny under NIS 2.

35.5%

of all breaches were
third-party-origin
(+6.5 % YoY)

41.4%

of ransomware/extortion
incidents started via
a supplier



32%

Healthcare breaches via suppliers

**One compromised
supplier = many
victims, letting
attackers earn more
with less work.**



46,7%

Energy incidents trace to suppliers



14%

Breaches from file-transfer vulns

NIS2

What you Must do about third-party providers ?

Article 21 - **Cybersecurity risk-management measures**

Member States shall ensure that essential and important entities take **appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.**

...

The measures referred to in paragraph 1 shall be based on **an all-hazards approach** that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

...

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

...

Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities **take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.** Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

NIS2

What you Must do about third-party providers ?



Supply-chain security policy

NIS 2 obliges you to document and evidence how you assess every direct supplier and their sub-suppliers, including secure-development practices.

All-hazards risk management including suppliers

Article 21 of the NIS 2 directive mandates that organizations implement an all-hazards approach to risk management, including their supply chain.

Multi-factor authentication for vendor access

All privileged or remote access—even from third-party support teams must use MFA authentication solutions.

Management liability and fines up to €10M or 2% of turnover

Article 26 of the NIS 2 directive imposes significant financial penalties and personal liability for non-compliance, up to €10 million or 2% of global annual turnover.

24-hour initial incident report

The NIS 2 directive requires organizations to report any significant cybersecurity incidents within 24 hours of their occurrence.

Beyond the checkbox: A five-step vendor security roadmap

1



Map & Tier your vendors

2



Assess and verify evidence

3



Contract controls

4



Monitor & Drill

5



Track & Improve

Step 1 - Map & Tier Vendors

- List clinical & IT suppliers

Identify and catalog all clinical and IT vendors that provide goods or services to the organization.

- Rank by Impact/Data

Assess and prioritize the vendors based on their level of impact on the organization's operations and the data they are processing

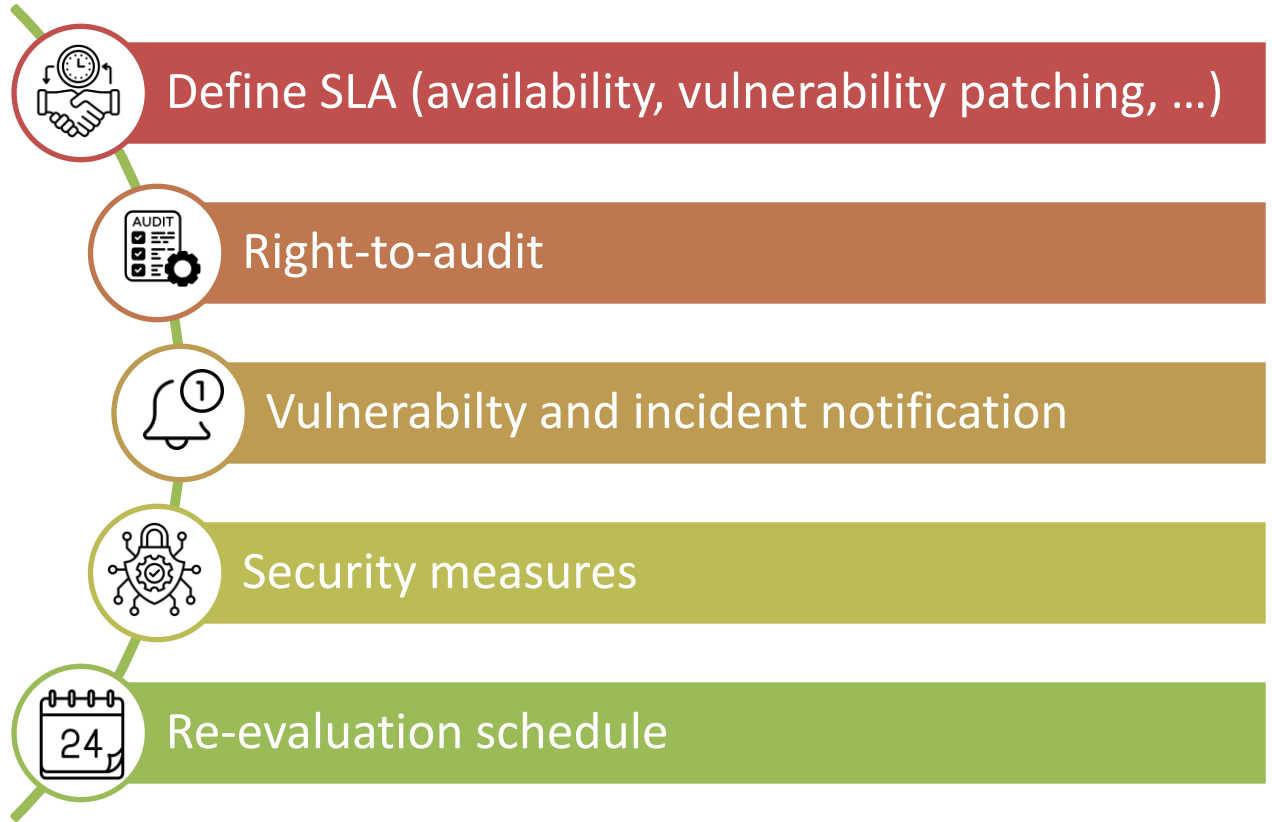
- Tier vendors

Based on the level of impact, assign a Tier to the vendors (e.g., Tier 1, Tier 2, Tier 3)

- Focus on most critical Tier and new projects

Concentrate the initial analysis and management efforts on the most critical vendors that have the highest impact. Focus also on new projects.

Step 3 - Contract controls



Step 4 - Monitor & Drill

Easy



Run weekly auto-scan of vendor's external attack surface



Send automated monthly 3-line security digest



Hold tabletop exercise with your critical vendors twice per year

Challenging





Quarterly Vendor KPI Dashboard

Metric	Target	Current Status	Trend
Automated external scan coverage (Tier 1 vendors)	100 %	100 %	— stable
Mean Time-to-Remediate (Tier 1 vendors)	< 24 h	18 h	▼ improved from 26 h
Critical patches applied in 14 days	≥ 95 %	91 %	▲ up from 85 %
High-severity vulns still open (Tier 1)	0	4	▲ up from 2
Vendors missing 24 h breach clause	0	3	▼ down from 7
New vendors assessed this quarter	—	5	— baseline
New vendors overdue questionnaire submission	0	2	— first measurement

Step 5 - Track & Improve

Pitfalls & Quick Wins (let's be honest about the pain points)

 Pitfalls	Practical, low-friction fix 
Gold-plating – we expect every vendor to be <i>more</i> secure than our own hospital.	Mirror principle: ask only for controls you already run or plan to run within 12 months; align maturity.
Custom checklist overload – every hospital invents a 200-question PDF; vendors drown.	Adopt the H-ISAC 10-control core + optional “delta” questions; everyone speaks the same language.
Endless questionnaire, no follow-up – 500 answers create 70 risks, none tracked.	Use an off-the-shelf tool to auto-score responses and push the top-5 risks into your cyber risk management tool / board.
Assessment = company-wide, project ignored – deployment-level risks unseen.	Run a project-risk review for every new rollout.
Supplier ghosting – no reply after three reminders.	“Silence =red” rule: after 30 days vendor status turns red in dashboard; procurement escalation kicks in.
Irrelevant certs – vendor sends ISO 27001 of its data centre only.	Request the SoA page ; must list controls operated by the <i>supplier</i> or it's rejected.
“Can't disclose—confidential” – blanket refusal to share evidence.	Offer a screen-share under NDA : vendor shows logs/pentest on-screen; no files leave the call.
Undefined 24 × 7 escalation path – no human to call at 02:00.	Contract a named cyber on-call number and test it .

What healthcare can borrow from banking/finance under DORA ?



1 Vendor concentration risk flag

Add “% care dependency” column in your vendor sheet; red if >30 %.

2 Threat-Led Red-Team incl. suppliers

Joint red-team with one Tier 1 vendor using.

3 Exit & substitution planning

Draft 1-page Plan B per Tier 1: data export format & restore test.

4 4th-party & sub-outsourcing visibility

Require sub-processor list; flag non-EU or non-ISO entities.

Your first 3 moves on monday

1

**Export last-year spend,
mark vendors we can't
survive 24h without**

Spot single-point failures
before the next board update

2

**Add a 24h breach-notice
clause
to the next contract**

Meets NIS2 Art 23
costs €0, scales to all suppliers

3

**Run a free Shodan scan
on one Tier-1 vendor**

5-minute check surfaces open
ports
shows an immediate win

Small steps, big resilience



Thank you

