



Choose Scandinavian trust

Cybersecurity in CE marking - An update

Geir Hørthe, Tore Ledaal
and Daniel Havre

2023-03-02

Agenda

Cyber security into CE marking

- Radio Equipment Directive
- Cyber Resilience Act

Practical approach

Q&A



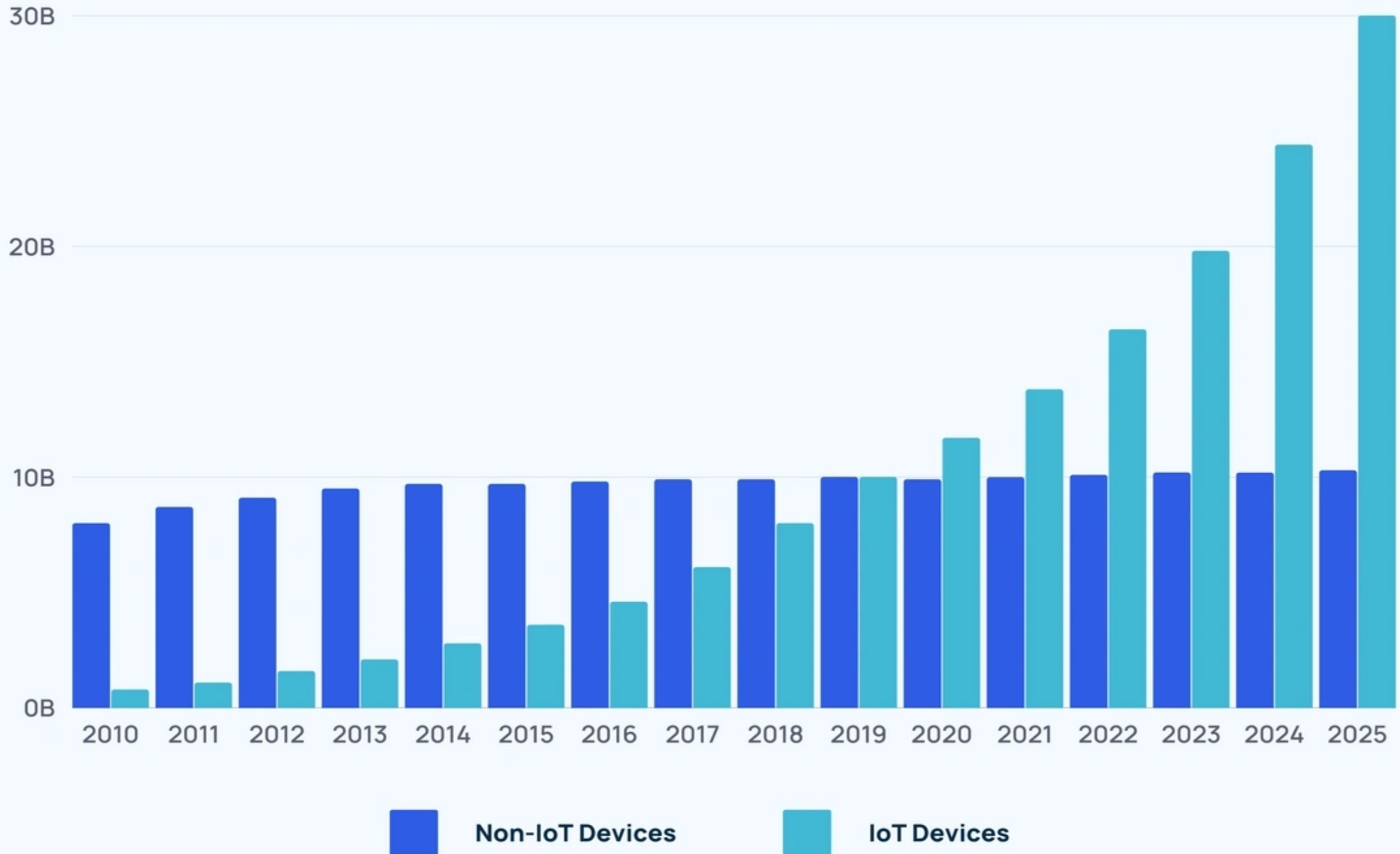
A smart house



> 50 connected devices in 1 house!



Non-IoT and IoT active devices from 2010 to 2025



Forbes – Cyber security trends 2023

IoT Attack Surface / Vulnerabilities



50 billion will be wirelessly connected via a network of sensors to the internet by 2021 (Cisco)

By 2023, there will be 3X more networked devices on Earth than humans

By 2025, an average connected person anywhere in the world will interact with connected devices nearly 4,800 times per day

Basically one interaction every 18 seconds. (IDC)

Security incidents involving IoT devices have impacted 67% of enterprises. (Forrester)

50% IoT devices on corporate networks security organizations don't maintain basic security measures beyond default passwords

98% of all IoT device traffic is unencrypted - exposing personal and confidential data on the network

Regulatory Schemes?

USA

Europe

Asia



CE marking focus – products on the market must be safe



- Safe from electrical shock and fire
- No Electromagnetic Compatibility (EMC) interference
- Well-functioning radio
- Energy efficient
- No toxics
- But no security requirements!

Safety by design



EU is introducing cyber security requirements

- Cyber Security Act
- Cyber Resilience Act
- Radio Equipment Directive

RED – Radio Equipment Directive

- Mandatory – CE marking
- Scope – most wireless products = most all IoTs
- Requirements for use of radio – and EMC and Safety
 - and now Cyber security
 - 1 August 2024
- 3 Cyber requirements



RED article 3.3



- d) not harm the **network** or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service
- e) incorporate safeguards to ensure that the **personal data** and privacy of the user and of the subscriber are protected
- f) radio equipment supports certain features ensuring protection from **fraud**

Radio Equipment Directive - Standards

Working on harmonised standards – 1 draft is published

- CENELEC aims for publication by 22 December 2023
- ETSI EN 303 645 – Consumer IoT

ETSI EN 303 645

- First international IoT cybersecurity standard
- Referred to in multiple countries world wide
- Coming into the CB certification scheme – from Nemko initiative.

RED: Additional requirements to ETSI EN 303 645

Some major change (from February RED draft standard)

- Defense of Denial of Service (DOS) attacks
- Ensuring that hardware contains no vulnerabilities
- Description of services which are exposed via network interfaces (Bluetooth, WiFi, etc)
- Logging requirements (Personal data))
- Supervisor/parental Access Controls (Children products with Personal data)
- 5G requirements likely to come (Personal data)

Majority of IoTs will face some additional requirements from RED, but already meeting ~75%)

* i) monetary transaction not considered, ii) the differences depends on the product



EU Cyber Resilience Act

EU Cyber Resilience Act

- Describes essential requirements
- Prescribes the use of CE marking
- Requires Declaration of Conformity and Technical File
- Describes obligations of Economical Operators like Manuf., Aut.repr., Imp., Dist.
- Market surveillance

EU Cyber Resilience Act

- Software bill of materials
- Requirement of keeping the product updated after putting on market i.e. updates to close vulnerabilities
- Reporting of active exploits of vulnerabilities
- Heavy fines for breaches (up to 15M EUR / 2.5% of rev)
- Scope
- Self declaration, but NB required for some products (e.g. industrial equipment)

EU Cyber Resilience Act

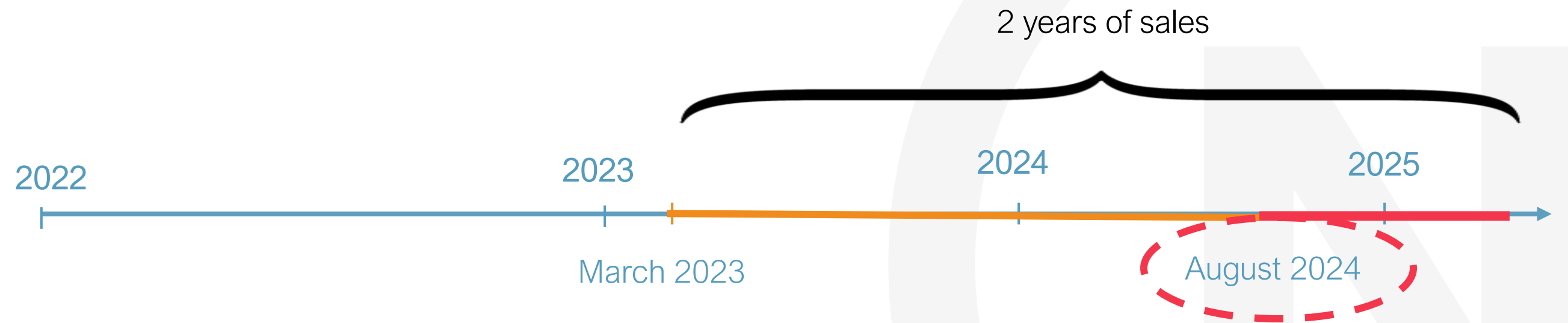
- Proposal
- 24-month transition period (12 month for reporting)
- Will replace cyber security requirements of RED
- But does not change current recommendations of RED
- 2026/2027?



How to work efficiently with cyber security

- Include cyber security into general compliance work from start.
- Do separate cyber security risk analysis
- Standardize cyber security solutions for multiple products (modules?)
- Use international standards to document security (as with safety, EMC etc.)
- Prepare well in advance for coming regulatory requirements, such as CE marking

Timeline implementation



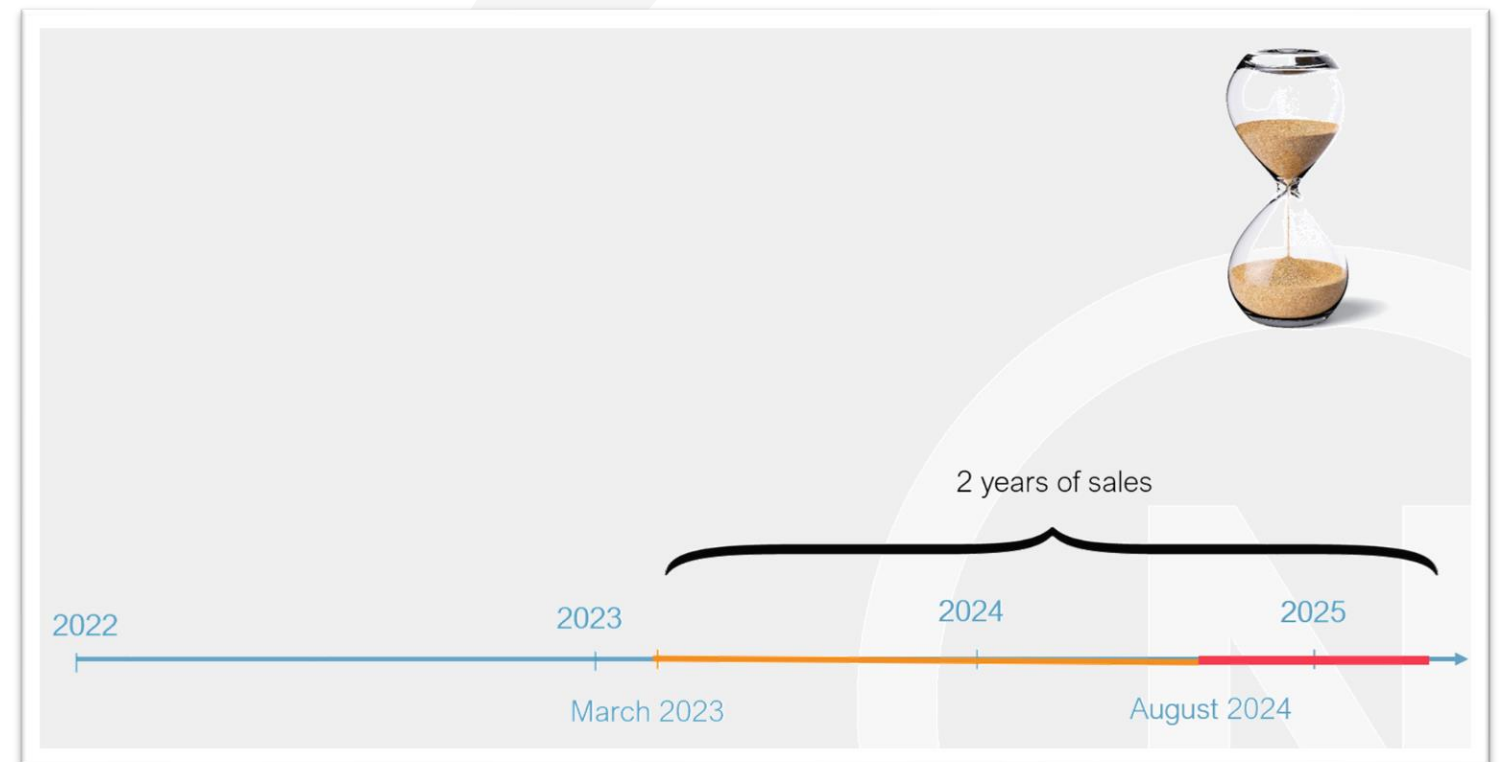
Challenge

A manufacturer plans to sell **the same** product after 1 August 2024, as they are today.

When does the product need to comply to the cyber security requirements?

Today!

If it does not comply today
- it will not comply next year



Practical questions

- Modules
 - What if RF module is certified?
 - What if network module is certified?
- What if IoT is behind a router, then no requirements?
- After 1 August 2024 – what about spare parts?
- How to demonstrate compliance to RED before harmonized standard?
- How to demonstrate compliance to RED after harmonized standard?
- What if no harmonized standard 1 August 2024?

Practical questions

- How will CRA remove the RED cyber requirements?
- What about RED and cyber security for wired products?
- Nemko perform
 - Gap analysis to ETSI std
 - Evaluations to ETSI stdWhat is the difference?
- I plan to stop selling products August next year – do I need to comply to RED cyber?
- I plan to continue selling my product after August next year – when does the product need to comply to RED cyber?



- Global cyber security requirements.
- RED puts cyber security into CE marking August 2024
- Required even if same product was also sold prior to this date
- Harmonized standards to come - relevant standards exists
- The Cyber Resilience Act – will expand the scope further for CE marking
- Recommended start: Gap analysis / Workshop covering current products

Summary

A hand is shown holding a white marker, writing the word 'Summary' in a cursive font on a light gray background.

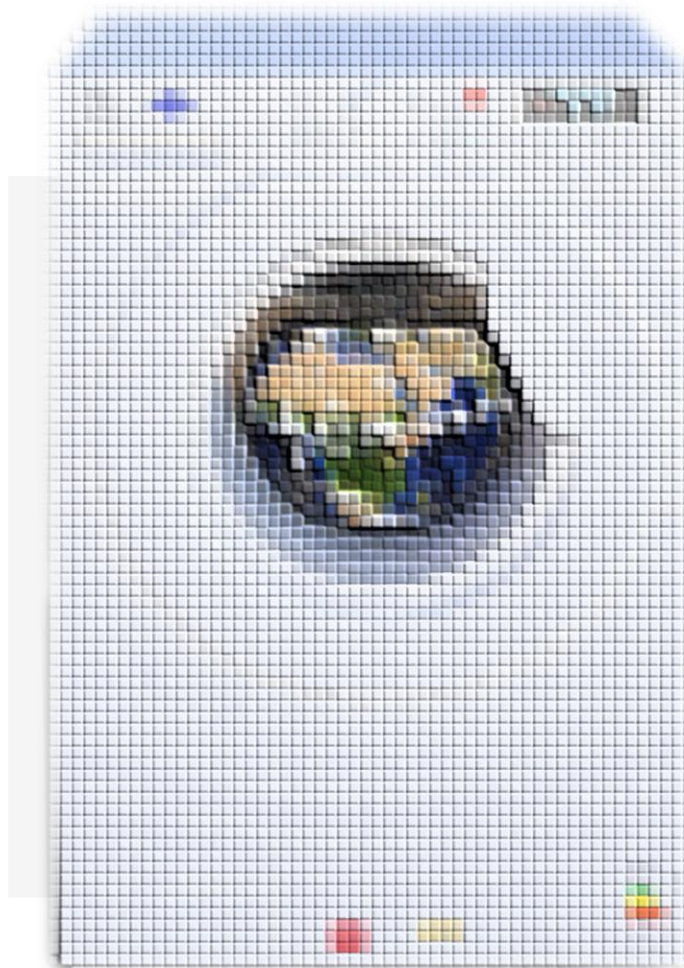
Examples of cyber security projects by Nemko

Products

- Household products
- Toys
- Routers
- Locks
- Phone system
- Lighting system
- Smart House
- Grid IoT
- EV charger

Projects

- Trainings
- Workshops
- Gap analysis
- Attestation
- Certification
- California regulation
- RED (gap analysis)



Prepared or not prepared

Already evaluated



or

Not evaluated



Are my products in the scope of RED cyber security?

- Book a complimentary 10 min assessment with us!
[Link to booking page](#)

