knowit

The nightmare scenario

knowit

Guest lecture – the NIS2 directive

A high common level of cybersecurity across the Union

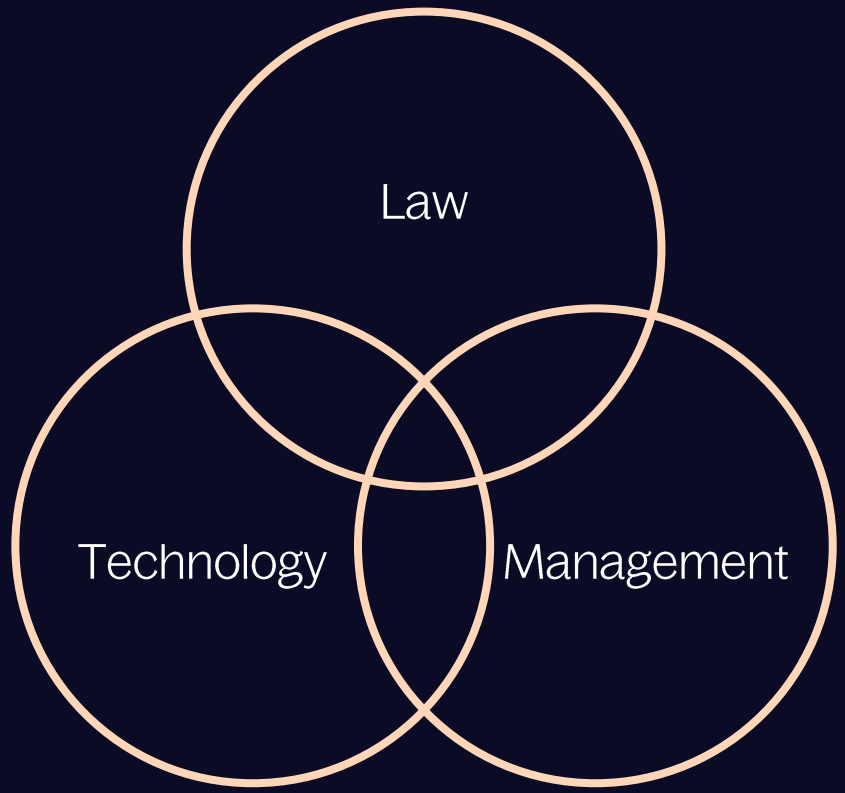
- what it is
- why it is important
- what is needed for compliance

knowit


A sustainable
and humane society
through digitalization
and innovation

Supporting clients'
digital transformation

Knowit Cybersecurity &
Law



knowit

Who we are

- Axel Törnqvist
- Legal counsel at Knowit Cybersecurity & Law

- Sara Öijerholm-Ström
- Legal counsel at Knowit Cybersecurity & Law

Agenda

Knowit Cybersecurity & Law – Department of Computer and Systems Sciences

1. Introduction to the Union legislation
2. General overview of cybersecurity legislation
3. Diving further into NIS2
4. Working with the legislation in practice
5. Questions

The legal system of the European Union

knowit

- Primary legislation – the treaties
- Secondary legislation – acts, directives, decisions etc.
- The primary legislation sets the boundaries for the what, when and how
- The secondary legislation is how the will of the primary legislation takes form

Regulating cybersecurity

Current NIS legislation

Protective Security Act

DORA

Sector-specific legislation

OVERARCHING PURPOSE OF THE ORIGINAL NIS DIRECTIVE

Ensuring the reliability and security of networks and information systems which services of economic and societal importance are dependent upon

The first NIS-directive

knowit

- Entered into force 2016
- Directives must be implemented in the respective member state

- National implementation – 2018
  - *The NIS Act*
  - *The NIS ordinance*
  - *General supplementary regulation from MSB*
  - *Sector-specific supplementary regulation*

knowit

Main legal obligations

Proactive obligations

- 11 § - maintaining a systematic and risk-based approach for governance of cybersecurity
- 12 § - conducting a risk analysis
- 13 § - *proportional* mitigating measures to minimise the risk of disruptions
- 14 § - *proportional* mitigating measures to minimise the effects of an incident

knowit

Main legal obligations

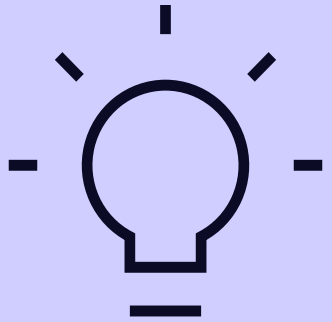
Reactive obligations

- 18 § - Reporting incidents to the national CSIRT
- Incidents shall be reported if a disturbance has a *significant impact* on the continuity of the service

- In Sweden the national CSIRT is MSB
- MSB has clarified what a *significant impact* entails in their guidance

Why do you think the NIS directive was updated?

Discuss with your neighbor!



Why NIS2?

Security of Network and Information Systems

To increase the Union's level of cyber resilience

1. Increase in threat levels
2. Dependence on essential services
3. Cross-border dependency
4. A digital transformation is hazardous without precaution
5. The implementation of NIS1 was fragmented and lacking in execution

knowit

Main provisions – an overview

- Systematic and risk based approach to cybersecurity
- Undertaking technical, operational & organisational risk management measures
- Reporting incidents
- Ensuring operational continuity despite incidents
- Senior management's level of responsibility

Expanding the scope

- Sectors of high criticality (Annex 1):
  - Energy
  - Transport
  - Banking
  - Financial market infrastructures
  - Health
  - Drinking water
  - Waste water
  - Digital infrastructure
  - ICT service management
  - Public administration
  - Space

knowit

Expanding the scope

- Other critical sectors (Annex 2):
  - Postal and courier services
  - Waste management
  - Chemicals
  - Food
  - Manufacturing
  - Digital service providers
  - Research

Harmonised approach for identification

knowit

- Main provision:

Operators qualifying as a medium-sized enterprise within an EU context

Medium sizes enterprize:

- Head count of 50-249
- Turnover ≤ €50 million
- Balance sheet total ≤ €43 million

Changing the nomenclature

knowit

Operators of essential services – Operators of digital services

Essential entities – Important entities

Transition from focusing on the provision of the critical service to the entities operations in its entirety

Please note: interpretation of entity should not necessarily be restricted to a legal entity

This is subject to a large degree of legal uncertainty

Why different roles?

Essential entities

- Generally viewed as more critical in terms of what an operational disruption would entail
- Subject to more scrutiny from supervisory authorities
- Heavier sanctions

Important entities

- Requirements for reporting not as onerous
- Solely reactive supervision
- On paper the legal requirements are comparable

knowit

Kahvitauko/Fika/Kaffepause

New legal obligations – A new directive!

The role of NIS2 – Ensuring continuity

- Proportionate *risk management* measures
- These entail some explicit examples within the legislation, but these are not exhaustive
- Examples include;
  - Established processes for incident management
  - Third party management
  - Use of encryption
  - Means of authentication

The role of NIS2 – Ensuring continuity

- Implementing measures to ensure continuity in case of disruptions
- Reporting obligations
- Cooperation with the competent authorities

New provisions – reporting

What to report:

- Incidents of significant impact
- Report to CSIRT or, when applicaple, competent authority

When to report:

- 24h – early warning
- 72 h – incident notification
- One month – final report

Or

If incident is still ongoing after one month, a progress report and then a final report

CSIRT can request status updates

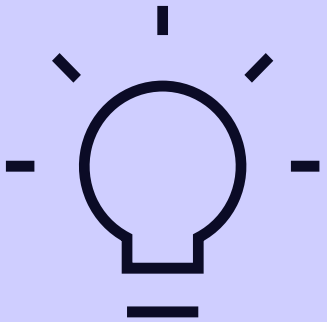
Emphasis on responsibility of senior management

- Members of the management bodies of essential and important entities are required to follow training
- The management bodies approve the cybersecurity risk-management measures, oversee its implementation and can be held liable for infringements
- Members of senior management may be prohibited to exercise their managerial function if they have proven to, intently or by gross negligence, not complied with the legal obligations

What do you think constitutes an incident of significant impact?

Discuss with your neighbor!

Focus on how you would codify circumstances into law that would necessitate reporting



An incident shall be considered to be significant if:

a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned

b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Commission implementing Regulation C(2024) 7151 for digital service providers can show us some further clearification

Consequenses of infringements

knowit

If a competent authority after supervisions find an entity to be in breach of NIS2 – the consequenses are to be proportionate and dissuasive,

Examples of aggravating circumstances to take into consideration:

1. If the entity has benefited economically which has lead to competitive advantages
2. Lacking cooperation during supervision
3. Cross-border effects

Cap for monetary sanctions

Essential entities

€10MM or

2% of global annual revenue.

Temporarily ban on an individual from holding management positions in case of repeated violations.

Important entities

€7MM or

1,4% of global annual revenue.

Other legal requirements

- NIS2 – only a part of the new cybersecurity compliance landscape
- *Lex generalis*
- DORA
- Protective security legislation
- CER

Time for practical application!

Lets apply the provisions for a healthcare-provider

knowit

Where do we begin?

- Applicability
  - Sector
  - Size of organisation
- Other legislation
  - Lex specialis
  - Onerous requirements
- Understanding the requirements
  - Security measures
  - Reporting
  - Redundancy
  - Awareness

knowit

What needs to be done?

- Perform a gap-analysis
  - Understanding where to begin
- Define actions
  - Delegation
- Follow-up
  - Verifying compliance level
- Redefine actions
  - And then we do it all over again

Compliance in practice

- Implementing ISO27001 for the Information Security Management System (”ISMS”) goes a long way
- Employing a risk-based approach for the legal requirements themselves
- Conveying both legal risk exposure as well as the benefits of an adequate security posture to the management body is of paramount importance in order to gain support from the whole organisation

A chain is only as strong as its weakest link

Knowit C&L

- If you are curious about what we do – visit Cybersecurity & law (knowit.eu) and read about:
- Our offering;
- Career opportunities and;
- Some interesting topics on our blog!

knowit

Tack/Takk/Kiitos