

Nordic region

Strengthening Cyber Governance Across the Nordic Region

PECB REGIONAL WEBINARS

Agenda

1. Who are the Nordics?
2. The Current Cybersecurity Landscape
3. Enhancing Cybersecurity Governance

Part 1

Who are the Nordics?

Key Characteristics - Happiness Index

The Nordics are ranked in the top 10 as the happiest places on Earth:

1. Finland: Ranked #1
2. Denmark: Ranked #2
3. Iceland: Ranked #3
4. Sweden: Ranked #4
5. Norway: Ranked #7

Key Characteristics - High voter turnout

High levels of engagement and participation in elections:

1. Faroe Islands (88%)
2. Sweden (84.2%)
3. Denmark 84.16%
4. Iceland (80.1%)
5. Norway 77.2%

Strong Digital Infrastructure

1. **High-speed broadband** and mobile connectivity (including 5G rollout) are widespread.
2. High levels of **digital literacy** across all age groups.
3. Nationwide adoption and use of **digital tools and services** in daily life (e.g., online banking, digital IDs, telemedicine).
4. Early adopters of d**igital identity systems** that ensure digitalization and interoperability of public services such as tax and health:

    - Sweden and Norway - BankID implemented in 2003 and 2004 respectively
    - Denmark - NemID was implemented in 2010 and replaced by MitID in 2021
    - Finland - Tupas introduced in 1999 supplanted by FTN in 2019.

High Levels of Digital Trust

1. 91 percent of Digital Post users are confident in communicating with public authorities using Digital Post.
2. 96.6% of the Danish population over the age of 15 have an active MitID.
3. 89% of users feel secure using MitID.
4. As of 2023, 5.2 million citizens receive Digital Post from public authorities.
5. 2.1 million powers of attorney have been granted since 2014.

NorwayNO

1

Oda (formerly Kolonial)

- **Sector:** Online grocery / Logistics
- **Service:** Scandinavia's largest online grocer.

2

Cognite

- **Sector:** Industrial AI / DataOps
- **Service:** data platforms for heavy-asset industries.
- https://www.cognite.com/en

3

Tibber (HQ in Norway, operations in Sweden)

- **Sector:** Energy
- **Service:** Smart energy consumption

SwedenSE

1

Spotify

- **Sector:** Music streaming (former unicorn)
- **Service:** One of Europe's most successful tech companies.

2

Klarna

- **Sector:** Fintech / Buy Now Pay Later (BNPL)
- **Service:** One of the largest private fintechs globally.

3

Einride

- **Sector:** Autonomous electric transport
- **Service:** self-driving electric trucks.

FinlandFI

1

Wolt (acquired by DoorDash)

- **Sector:** Food delivery
- **Service:** Food delivery in 38 countries

2

Aiven

- **Sector:** Cloud services
- **Service:** AI-ready open-source data platform

3

ICEYE

- **Sector:** Space tech / Satellite imaging
- **Service:** Synthetic aperture radar (SAR)

Icelandis

1. **Controlant**
   - **Sector:** Supply chain / IoT
   - **Service:** pharma supply chain optimization

2. **Kerecis**
   - **Sector:** Biotech
   - **Service:** Fish skin based wound **care**

3. **SnerpaPower**
   - **Sector:** Energy
   - **Service:** Efficient energy management

DenmarkDK

1. **Lunar**
   - **Sector:** Fintech / Neobank
   - **Service:** Digital banking platform

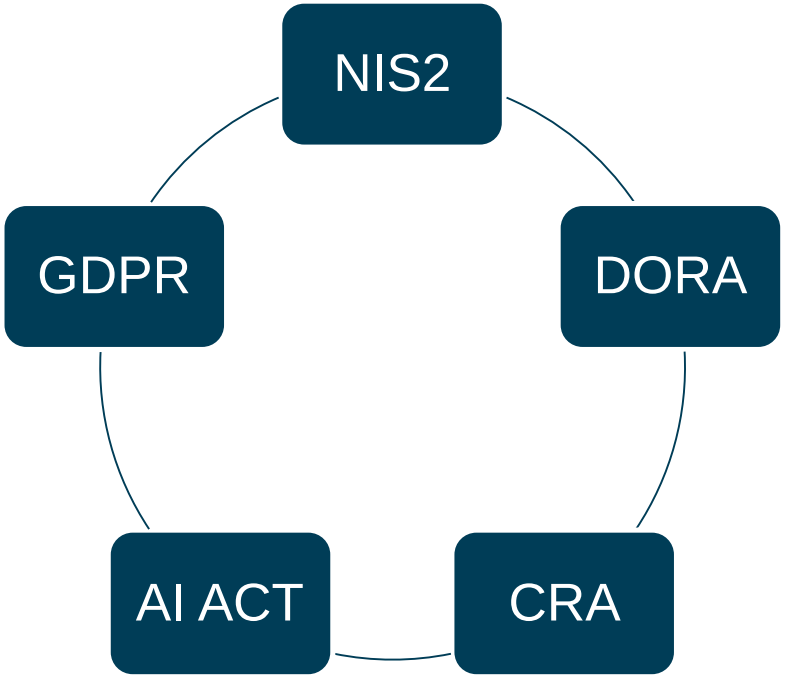
2. **Too Good To Go**
   - **Sector:** Food tech / Sustainability
   - **Service:** reducing food waste

3. **Trustpilot**
   - **Sector:** Review platform
   - **Service:** Global customer review platform

Part 2

Current Cybersecurity Landscape

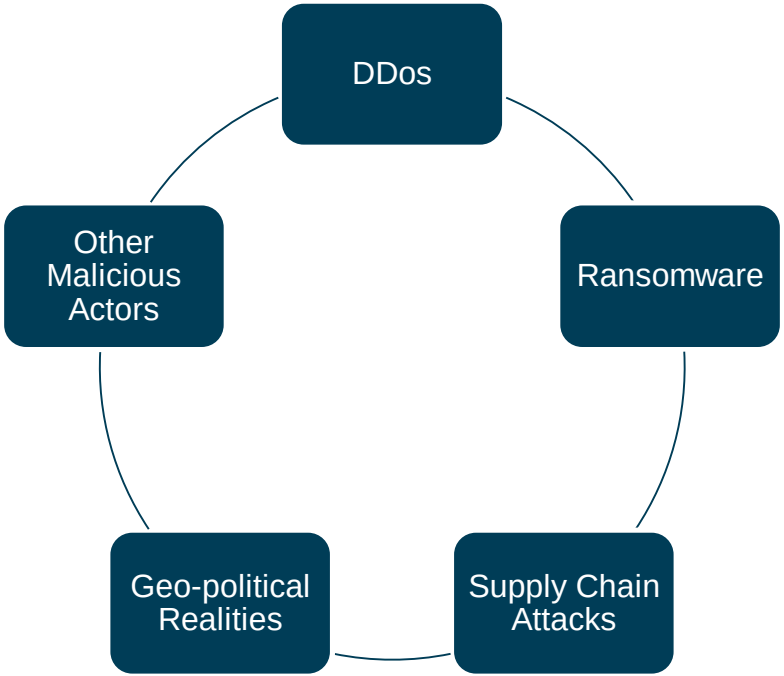
Legislative Impact



Commonalities within EU Legislation

1. Governance Focused
2. Risk based approach
3. Incident Management & Reporting
4. Supply Chain Management
5. Information Sharing

Dynamic Threat Landscape



Distributed Denial of Service

1. Swedish Bank-ID Service Hit by DDoS Attack, No Data Compromised
2. Update on Nordea's technical issues affecting our digital services
3. Danish Municipality Websites Down with a DDoS attack

Ransomware

1. Threat From Criminal Campaigns Affecting Maritime Entities In Nordics High
2. CloudNordic loses most customer data after ransomware attack
3. Nordic Choice Hotels Confirm Ransomware Attack

Supply Chain Attacks- Centre for Cyber Defense

1. Some suppliers make attractive targets for hackers as they constitute a single point of entry to multiple targets and data.

2. Some hacker groups have the capabilities and intention to attack suppliers that provide key services and infrastructure to companies and authorities in Denmark.

3. The Centre for Cyber Security CFCS assesses that this attack method is used by foreign states and cyber criminals.

Geo-political realities

1. Finland & Sweden apply for NATO membership in 2022
2. Finland becomes a member in 2023 followed by Sweden in 2024
3. Nordic countries have provided extensive support for Ukraine
4. Sabotage of cables in the Baltics
5. Suspected disinformation campaigns

Other Malacious Actors

1. Nation-State Actors
2. Cyber-criminals
3. Hacktivists
4. Insider Threats
5. Dark Web

Part 3

Enhancing Cybersecurity Governance

The Nordic Council

1. Protection of critical infrastructure
2. Cyber hygiene and awareness
3. Cross-border crisis coordination
4. Joint Cybersecurity trainings and simulations
5. International Cooperation

Focus Areas

1. Boards & Senior Management
2. Small and Medium Enterprises
3. Educational institutions
4. The General Public

Boards & Senior Management

1. Mandate
2. Resourcing
3. Roles & Responsibilities
4. Cybersecurity Risk Management

Small & Medium Enterprises

1. Resourcing
2. Creation of Nordic certification scheme or adopt UK Cyber Essentials
3. Funding
4. Management of sub-suppliers

Educational Institutions

1. Mandate
2. Understanding the role of cybersecurity within various industries and sectors
3. Budgets/Resourcing
4. Stakeholder management
5. Project and Program management design and implementation

The General Public

1. Public Service Announcements
2. TV Shorts/Animated Short
3. Social media campaigns targeting the elderly
4. Social media campaigns targeting teens
5. Project and Program management design and implementation

Key Considerations

1. Cybersecurity governance leadership has the appropriate mandate to effectively manage cyber risk
2. Ensure the board is educated on cybersecurity risk management
3. Consider the implementation of an ISMS based on ISO 27001 and/or BCMS based on ISO 22301
4. For SME's determine whether the adoption of UK Cyber Essentials or similar framework fits
5. Manage supply chain risk on a continuous basis in accordance with best practices

Q&A Session



Contact

- Email: geoffreylloydtaylor@icloud.com

For any questions or comments you can contact us below:

- support@pecb.com