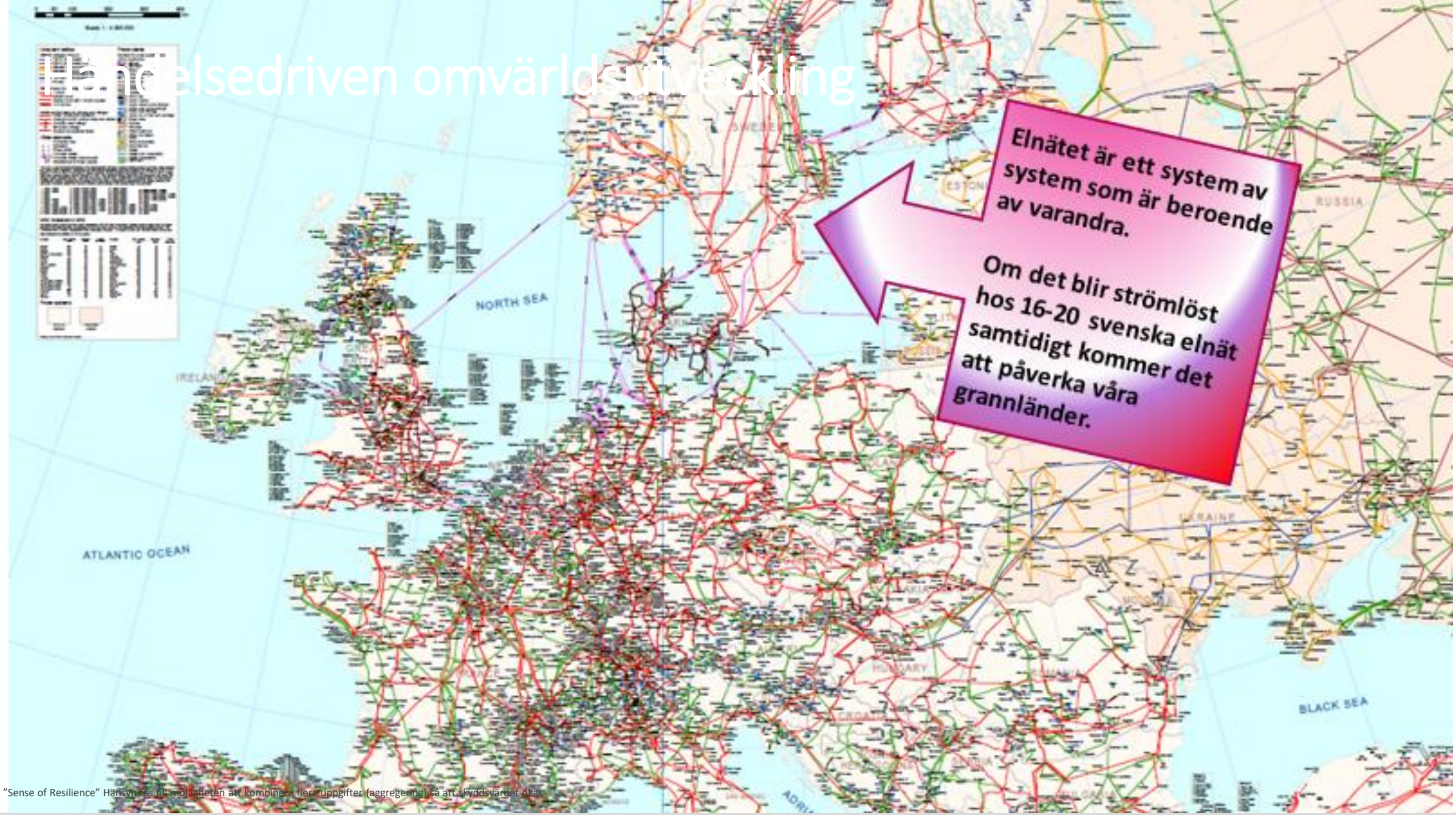
Strategi för säkerhet

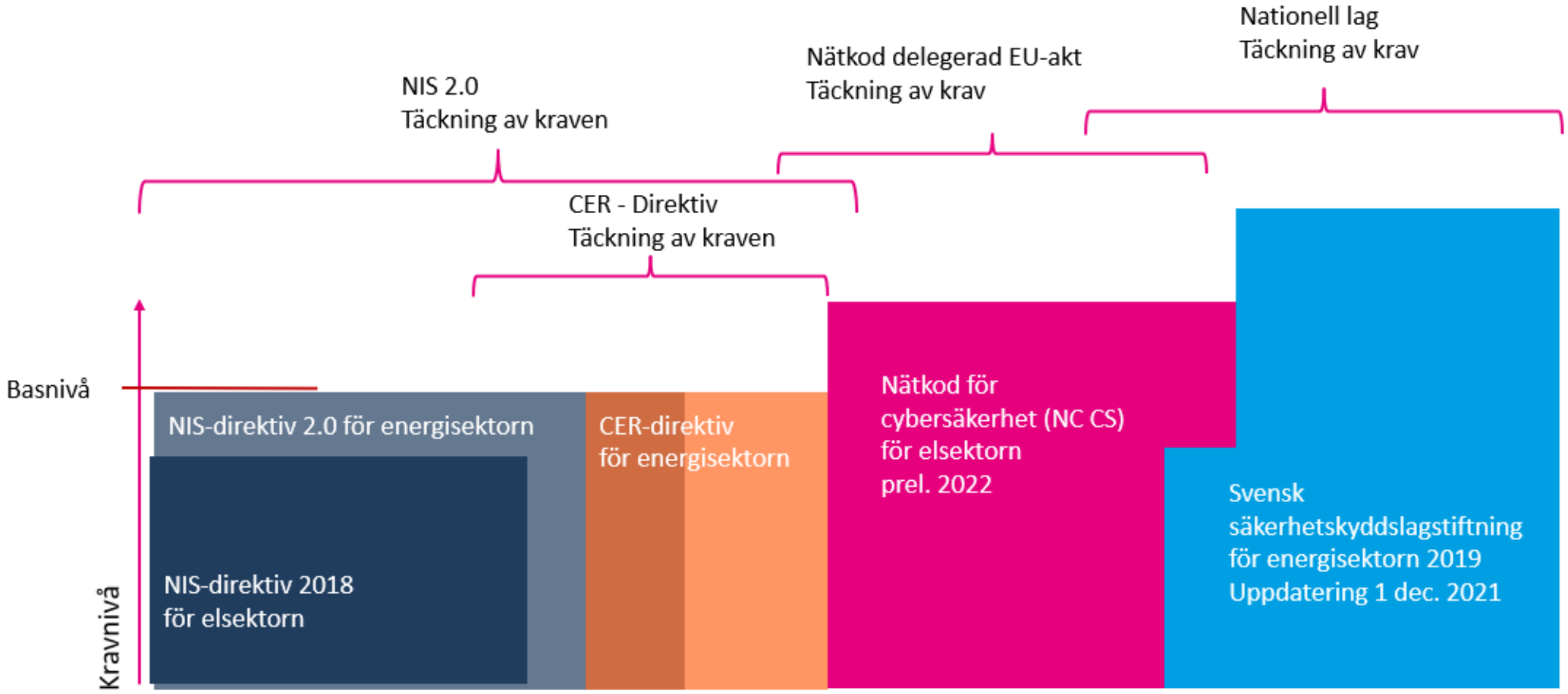
Anders Åhlgren, Jönköping Energi
Per Ahlström, Göteborg Energi
Annelie Rickardsson, Kungälv Energi
Emma Johansson, Energiföretagen

Händelsedriven omvärldsutveckling



”Sense of Resilience” Hänsyn tas till möjligheten att kombinera flera uppgifter (aggregering) så att skyddsvärdet ökar.

Legala säkerhetskrav



Ex. på specifika säkerhetsföreskrifter för energisektorn: NIS-föreskrift (STEMFS 2021:3), Incidentrapportering (MSBFS 2018:9)
Föreskrifter och allmänna råd om säkerhetsskydd (SvKFS 2019:1)

Strategi för säkerhet

- Strategin syftar till att stödja energiföretagens ledning med frågor kopplat till säkerhet.
- 7 punkter ger dig nycklarna till ett systematiskt och strukturerat säkerhetsarbete.
- Din verksamhets kultur avgör om säkerhetsarbetet lyckas!

Syfte och mål med strategin

Syfte:

- Tillämpning – direkt – oavsett vilken verksamhet du bedriver inom energisektorn

Mål:

- Säkerhetsarbetet stödjer affären i alla lägen
- Skapa resiliens: undvika störningar men också ha förmåga att snabbt återhämta när något sker

Målgrupp:

- Verksamhetsansvarig

Vad behöver vi göra? - minsta gemensamma nämnarna

1. **Genomför en ”Business Impact Analysis”** – hantera risker medvetet genom att undvika – lindra – överföra - acceptera - eller ignorera risken.

2. **Genomför en riskanalys** – som syftar till att visa vilka cyberhot och sårbarheter som finns mot företaget.

3. **Uppfyll informationssäkerhetskrav** – som omfattar bland annat dokumentation, klassning och spårbarhet. Skapa ett ledningssystem för informationssäkerhet (LIS) med roller och ansvar.

4. **Vidta säkerhets- och skyddsåtgärder** – skydda nätverk- och informationssystem. Inför säkerhetsåtgärder som antingen sänker ett riskvärde eller uppfyller ett informationssäkerhetskrav samt utbilda personalen "Social engineering".

5. **Förebygg incidenter** – genom härdning av utrustning samt utbildning och övningar med ständiga förbättringar. ”Security by design”.

6. **Monitorera hot och dela information** – att kunna rapportera incidenter "*Responsibility to share*".

7. **Ha bra ordning på kritiska resurser och tillgångar samt sårbarheter.** Följ upp!

Säkerhet är inte ledningens problem – TILLS DET ÄR DET!

Hisspitch!