# Appendiks 3. Bestyrelsesansvar og business judgment rule

**Ansvar**

- Bestyrelsesmedlemmer kan ifalde ansvar for utilstrækkelig risikostyring og sikkerhedsbrud.

**Business judgment rule**:

- Om der foreligger erstatningsansvar for (utilstrækkelig) risikostyring og sikkerhedsbrud bedømmes bl.a. efter "the business judgment rule".
- Business judgment rule er en uskreven regel, som indebærer, at hvis et ledelsesmedlem har truffet en beslutning, som beror på et forretningsmæssigt skøn, så bør ledelsesmedlemmet ikke ifalde erstatningsansvar, selv om beslutningen viser sig at være tabsforvoldende. Dette er dog kun gældende, hvis skønnet hviler på et ***forsvarligt beslutningsgrundlag***.

**"Forsvarligt beslutningsgrundlag"**

- For at sikre et "forsvarligt beslutningsgrundlag" til risikostyring indenfor cyber- og informationssikkerhed skal bestyrelsesmedlemmer tilvejebringe nødvendige oplysninger til at sikre passende og forholdsmæssige tekniske og organisatoriske foranstaltninger, herunder fornødne procedurer til risikostyring, se f.eks. vejledningens s. 6 og selskabslovens §115.
- Hvad der er forsvarligt, nødvendigt og tilstrækkeligt for den enkelte bestyrelse beror på en konkret vurdering ud fra de samlede omstændigheder, herunder afhængig af virksomhedens risikobillede, branche, produkter, størrelse, kompleksitet mv.
- Som generel retningslinje anbefales det at starte med at bruge anbefalingerne, checklisten og værktøjskasserne på s. 8-15 i denne vejledning ud fra "følg eller forklar" princippet.
- Eksempler på ***utilstrækkelige*** forhold, der efter omstændighederne potentielt kan være ansvarspådragende, er vist i boksen til højre.

**Forhold, der potentielt kan være ansvarspådragende:**

- Cyber er ubehandlet på bestyrelsesmøder
- Bestyrelsen har ikke dialog med relevante eksperter
- Bestyrelsen fastlægger ikke risikoappetit indenfor cyber- og informationssikkerhed
- Bestyrelsen giver ikke instruks til ledelsen
- Bestyrelsen modtager ikke træning
- Der er ikke et klart organisatorisk ansvar for cyber
- Forsyningskæden (supply chain risk) er ikke del af risikovurdering og -håndtering
- Virksomheden har ikke grundlæggende it-foranstaltninger på plads, f.eks. regelmæssig back-up eller regelmæssige sikkerhedsopdateringer (patching) af programmel
- Godkendelse af en stor infrastrukturoutsourcing – uden at tænke cyber ind

**Området udvikler sig løbende over tid, og et ansvar skal bedømmes konkret ud fra de samlede omstændigheder**