> DKCERTs trusselsvurdering for uddannelsessektoren

DKCERT

Trusselsvurdering

at bestemme troværdigheden og alvoren af en potentiel trussel såvel som sandsynligheden for, at truslen bliver en realitet

Trusler + sårbarheder = risici

DKCERT

Efterretningstjenester

Større sikkerhedsfirmaer

Store virksomheder

DKCERT

DKCERT

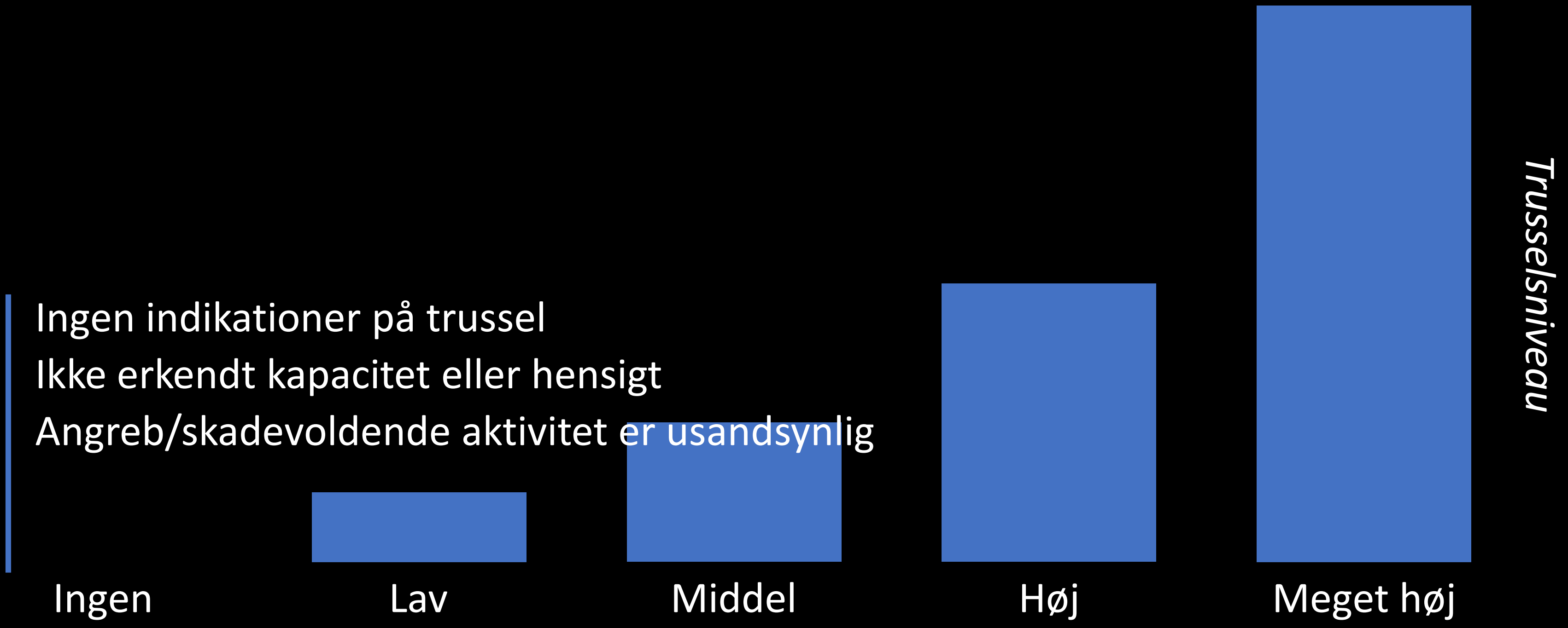
Identifikation

Indledende vurdering

Styring

Opfølgende vurdering og planlægning

DKCERT

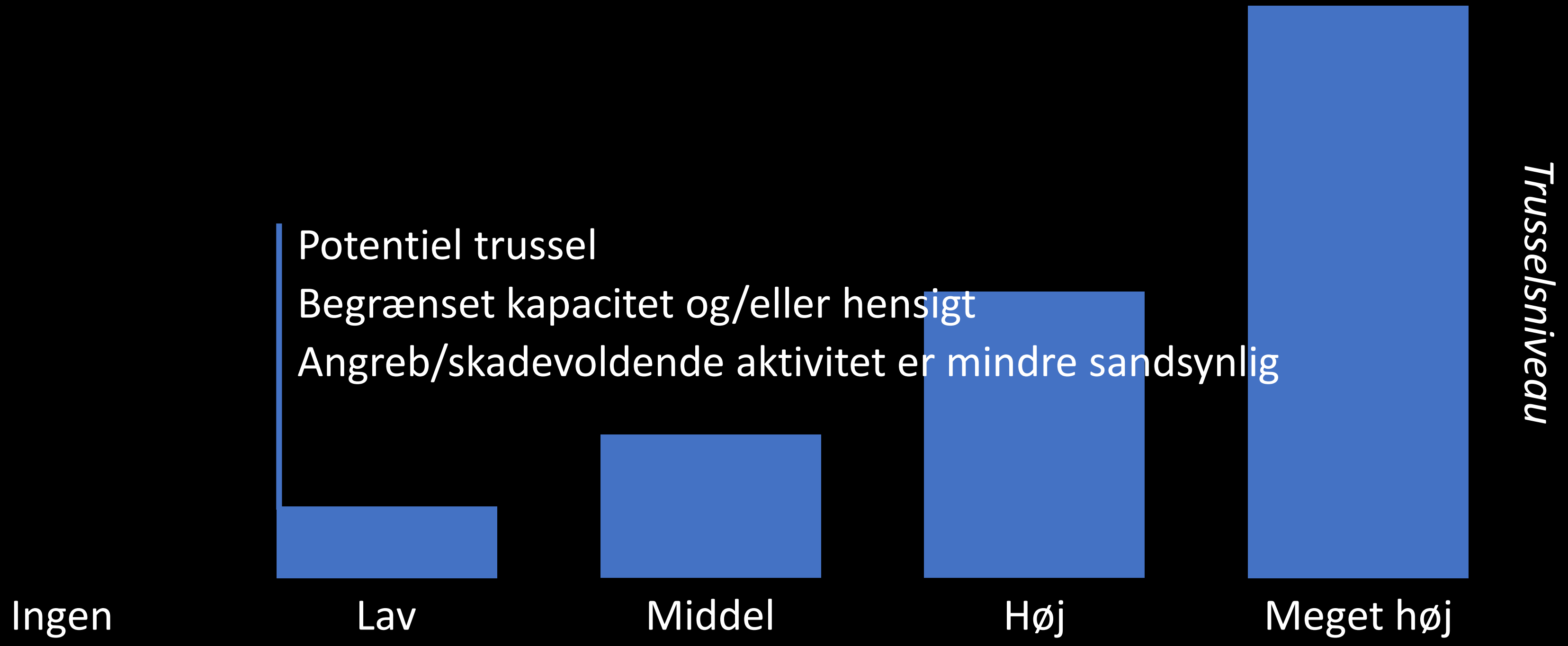


Ingen indikationer på trussel

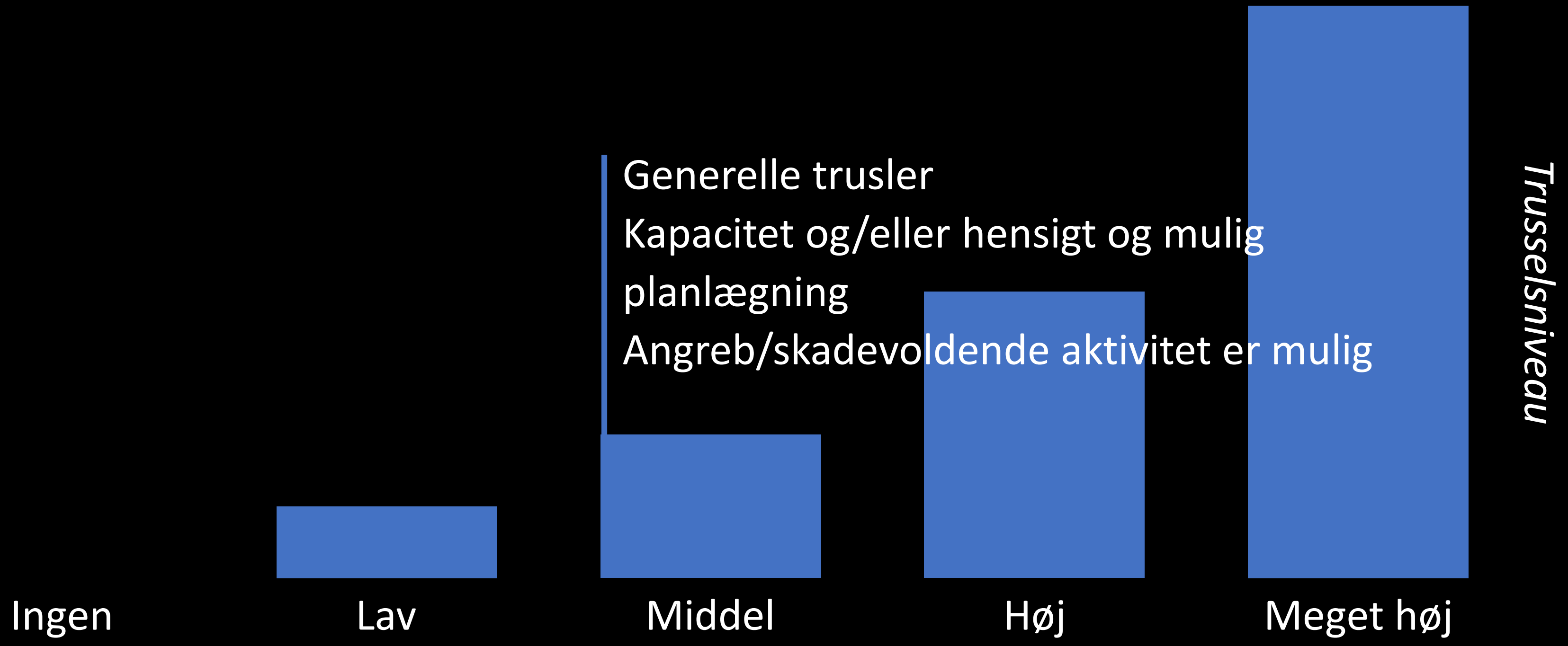
Ikke erkendt kapacitet eller hensigt

Angreb/skadevoldende aktivitet er usandsynlig

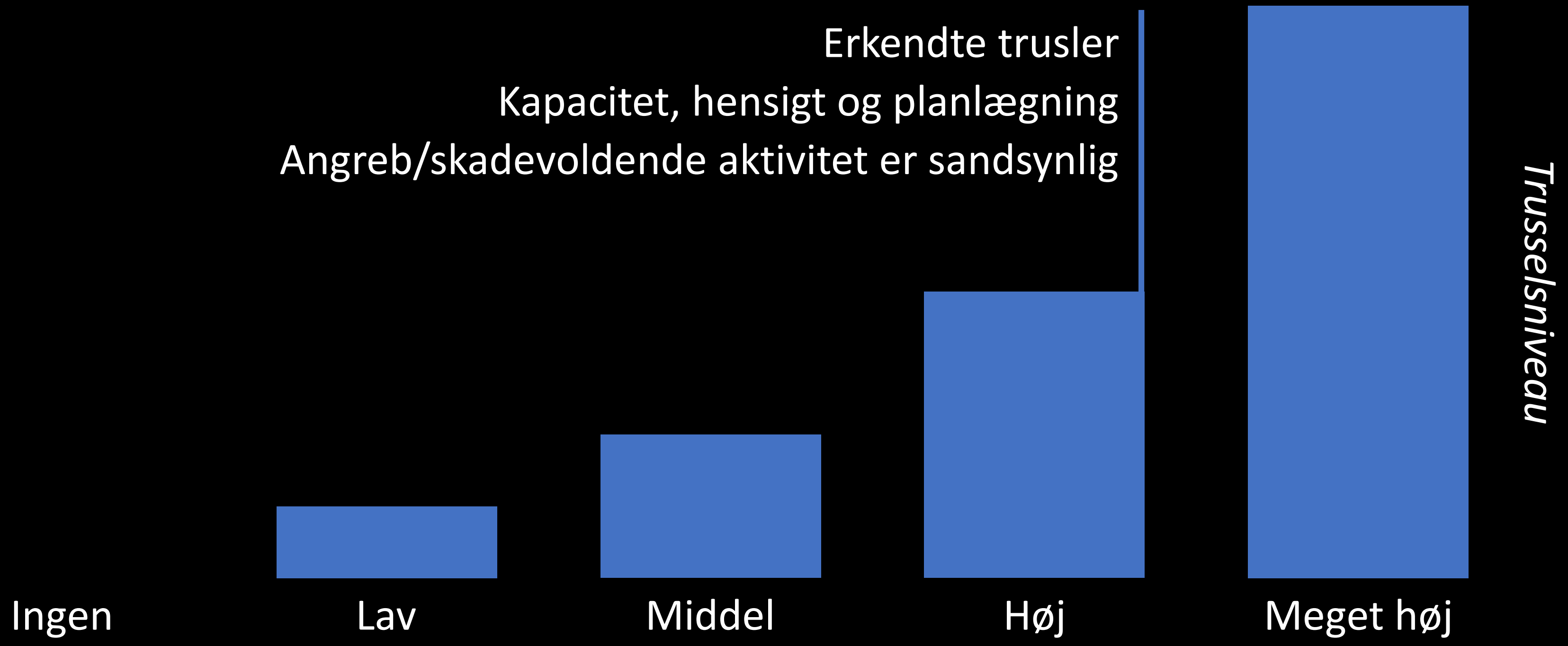
DKCERT


Potentiel trussel
Begrænset kapacitet og/eller hensigt
Angreb/skadevoldende aktivitet er mindre sandsynlig
Trusselsniveau
Ingen
Lav
Middel
Høj
Meget høj

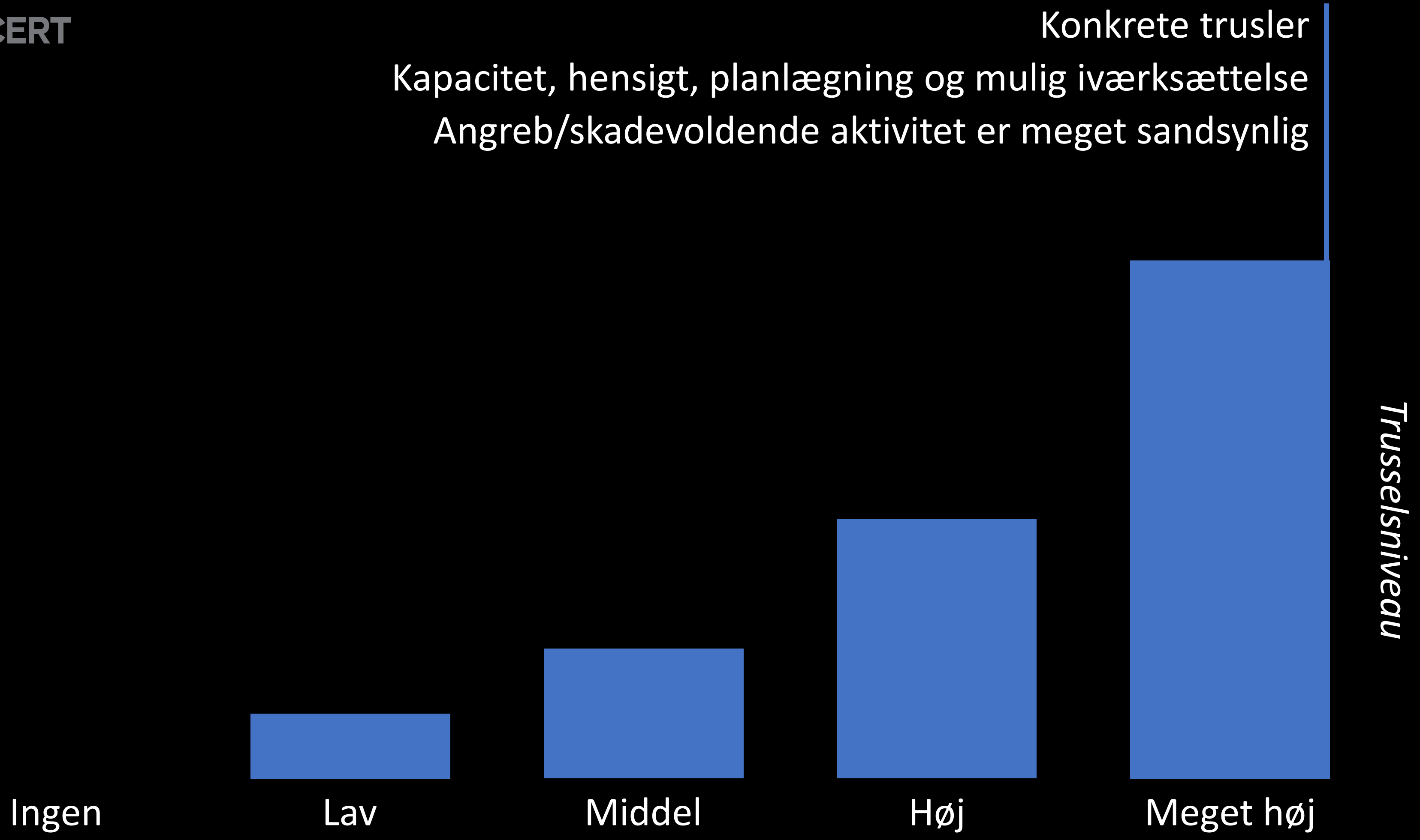
DKCERT


Generelle trusler
Kapacitet og/eller hensigt og mulig planlægning
Angreb/skadevoldende aktivitet er mulig
Ingen
Lav
Middel
Høj
Meget høj
Trusselsniveau

DKCERT


Erkendte trusler
Kapacitet, hensigt og planlægning
Angreb/skadevoldende aktivitet er sandsynlig
Trusselsniveau
Ingen
Lav
Middel
Høj
Meget høj

DKCERT


Konkrete trusler
Kapacitet, hensigt, planlægning og mulig iværksættelse
Angreb/skadevoldende aktivitet er meget sandsynlig
Ingen
Lav
Middel
Høj
Meget høj
Trusselsniveau

DKCERT

Interne kilder

Indberetninger

Phisningkampagner

Sårbarhedsscanninger

DPO-netværk og -tjeneste

DKCERT

Eksterne kilder

Trusselsstjenester, -sites, nyhedssites

CERT-netværket og MISP

Shadowserver

CFCS

DBIR

DKCERT

Trusselsvurdering

cyberspionage

cyberkriminalitet

cyberaktivisme

destruktive cyberangreb

insidertruslen

DKCERT

Meget høj trussel

cyberspionage

Målrettede spear phishing angreb
Password Spray Attacks
Kompromitterede studenter- eller ansattes konti
Iransk-baseret angrebsforsøg
FBI undersøgelse
Leverandørvinklen

DKCERT

Meget høj trussel

cyberkriminalitet

Ransomware er udbredt blandt organisationer og privatpersoner

Kryptominers

DDoS

Business E-mail Compromise

DKCERT

Lav trussel

cyberaktivisme

Defacement af hjemmesider
DDoS angreb
Andre metoder, der skal forstyrre

DKCERT

Mindre sandsynligt

destruktive cyberangreb

Ødelæggelse af digital infrastruktur eller fysisk infrastruktur, der understøtter den digitale

DKCERT

Meget høj trussel

insidertruslen

Insider med legitim adgang, som bevidst eller ubevidst påvirker uddannelsesinstitutionens virke

Der er to typer insiders, den bevidste og den ubevidste

DKCERT

Meget høj trussel

- den bevidste insider

80%* af bevidste insiderhandlinger anspores af arbejdsrelaterede hændelser

*Carnegie Mellon University

DKCERT

Meget høj trussel

- den ubevidste insider

Medarbejdere, som på grund af uklare eller manglende sikkerhedspolitikker eller manglende uddannelse ubevidst bryder organisationens sikkerhedspolitikker

En særlig gruppe ubevidste insidere er de uagtsomme medarbejdere, som undlader at følge gældende sikkerhedsprocedurer, fordi de føles besværlige eller unødvendige

DKCERT

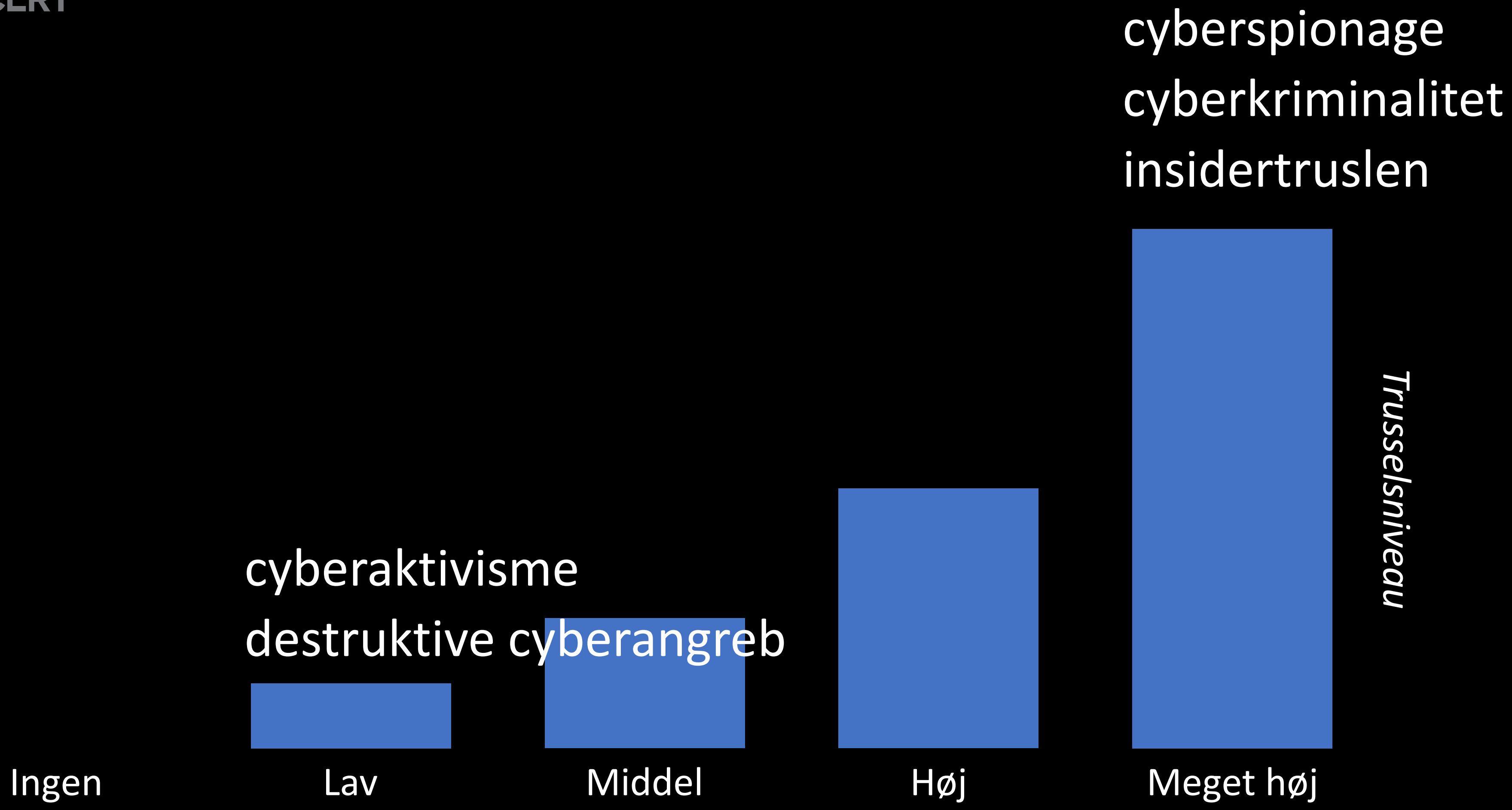
Meget høj trussel

Insidertruslen

Det er manglede awareness vedrørende truslen og konsekvenserne heraf, der er det største problem i forhold til insidertruslen.

Manglende awareness øger sandsynligheden for menneskelige fejl, uanset om disse er bevidste eller ubevidste.

DKCERT



cyberspionage
cyberkriminalitet
insidertruslen
cyberaktivisme
destruktive cyberangreb
Trusselsniveau
Ingen
Lav
Middel
Høj
Meget høj

DKCERT

[Spørgsmål?]