

Beredskapsøvelser for IT-sikkerhet

Maria Bartnes Line og Nils Brede Moe

maria.b.line@sintef.no

nils.b.moe@sintef.no

God og effektiv hendelsehåndtering krever:

- Kryssfunksjonelle, selvstyrte team
- Evnen til å lære

Hvorfor må vi øve på å håndtere IT-angrep?

Hendelser er komplekse

Hvorfor må vi øve på å håndtere IT-angrep?

Effektiv håndtering begrenser konsekvensene

Hvorfor må vi øve på å håndtere IT-angrep?

IT-sikkerhetshendelser og målrettede angrep
er høyaktuelle trusler

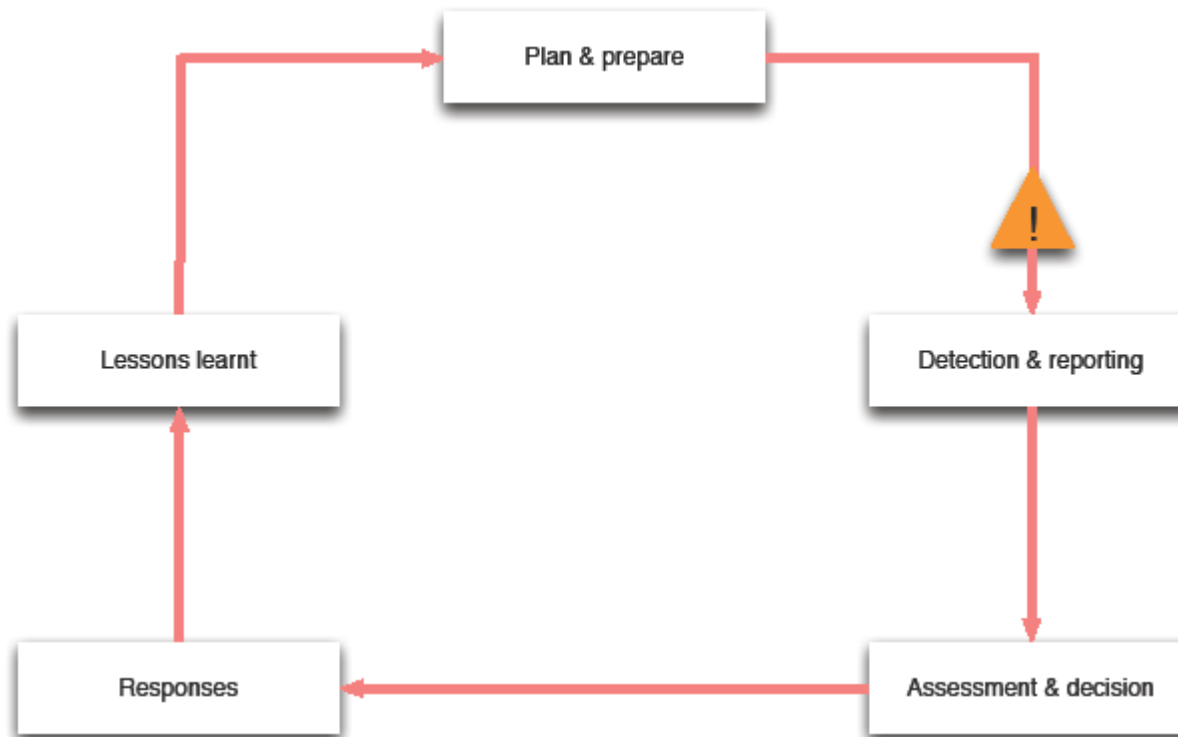
*”There are too many other tasks, so we haven’t had the time for it.
Maybe that’s wrong, not to prioritize it.”*

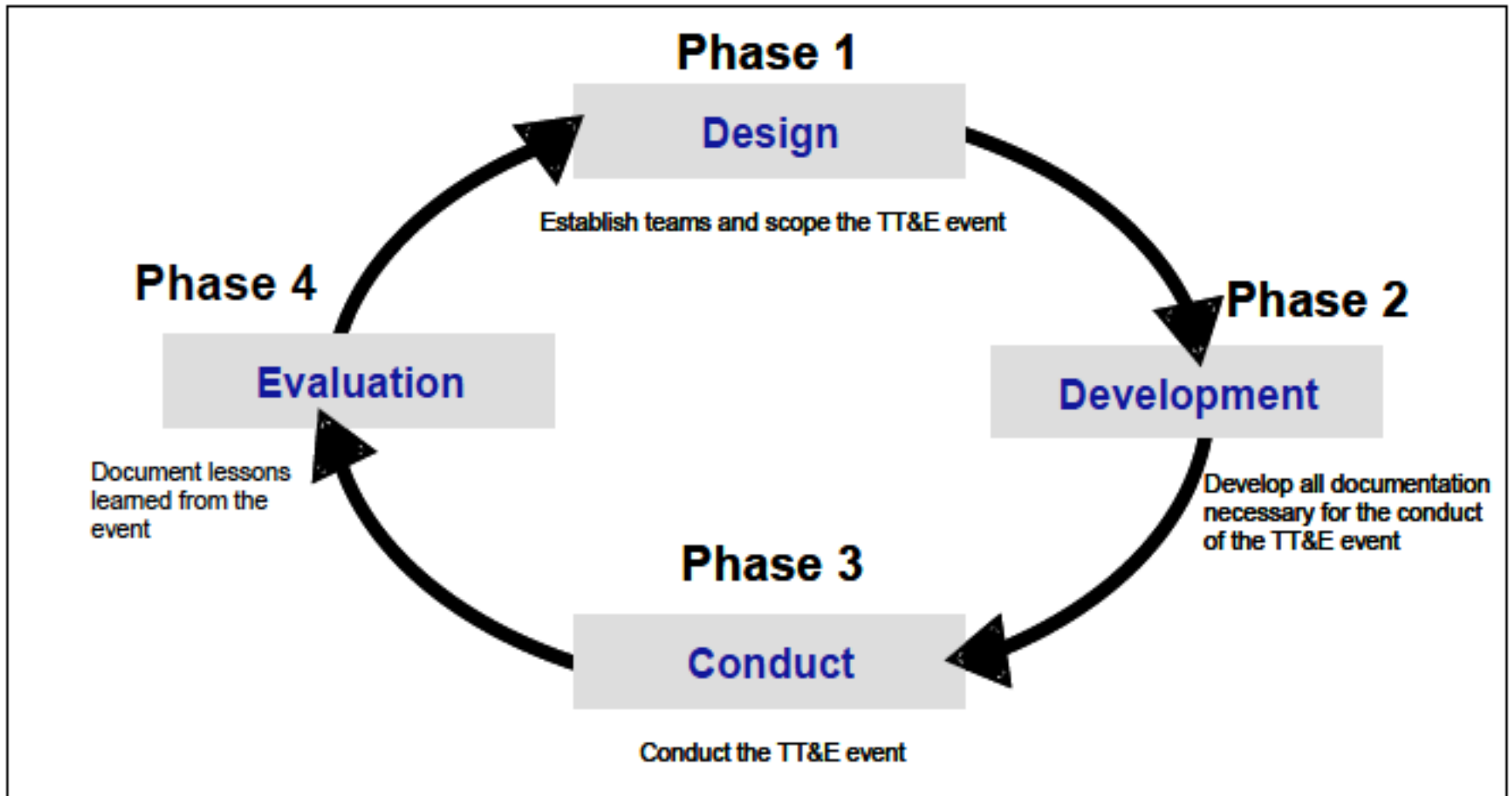
Control system manager in a large DSO

”As long as there has been no major attacks against the power industry in Norway, we consider the probability of an attack to be low. As soon as something happens, we will consider the probability to be increased.”

*Control manager in a large DSO
(before the Dragonfly attack)*

ISO/IEC 27035 – Information security incident management





Fra NIST SP 800-84: Guide to Test, Training and Exercise Programs for IT Plans and Capabilities

Øvelser

En veiledning i planlegging og gjennomføring
av øvelser i NVE

53
2013



R
A
P
P
O
R
T

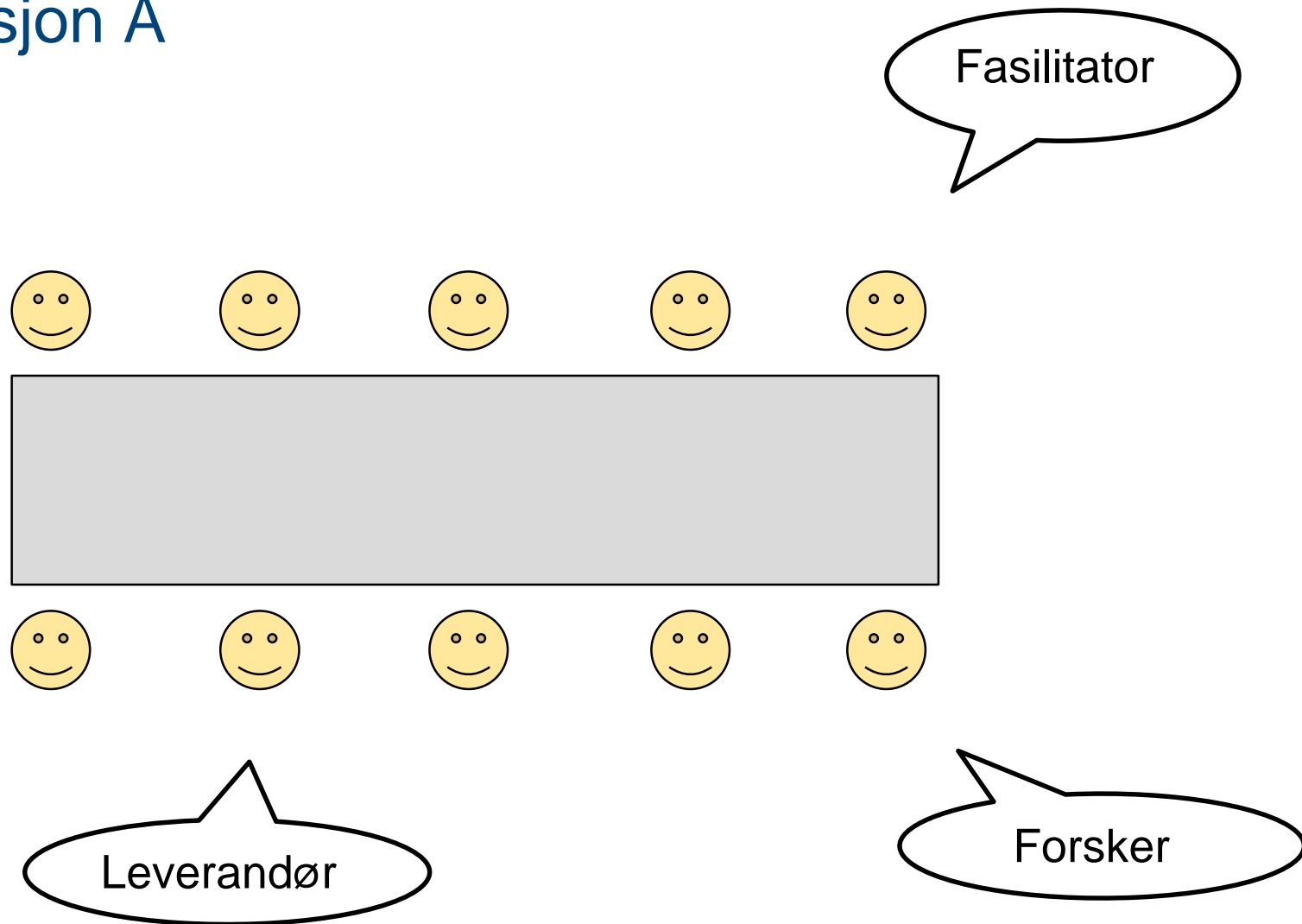
Observasjonsstudie av skrivebordsøvelser

- Hvilke utfordringer møter selskapet under gjennomføring av øvelsen?
- Hvordan kan disse utfordringene påvirke en reell hendelsehåndteringsprosess?
- Hvordan kan disse utfordringene imøtekommes under en øvelse?

Scenario i fem faser

1. Unormalt mye trafikk ut fra nettverket
2. To uker senere: SCADA-leverandør vil patche
3. Tre mnd etter første fase: strømløst i ett område, men ingen alarm
4. Strømløst i flere områder, fortsatt ingen alarmer
5. Mobilnett og Internett har falt ut

Organisasjon A

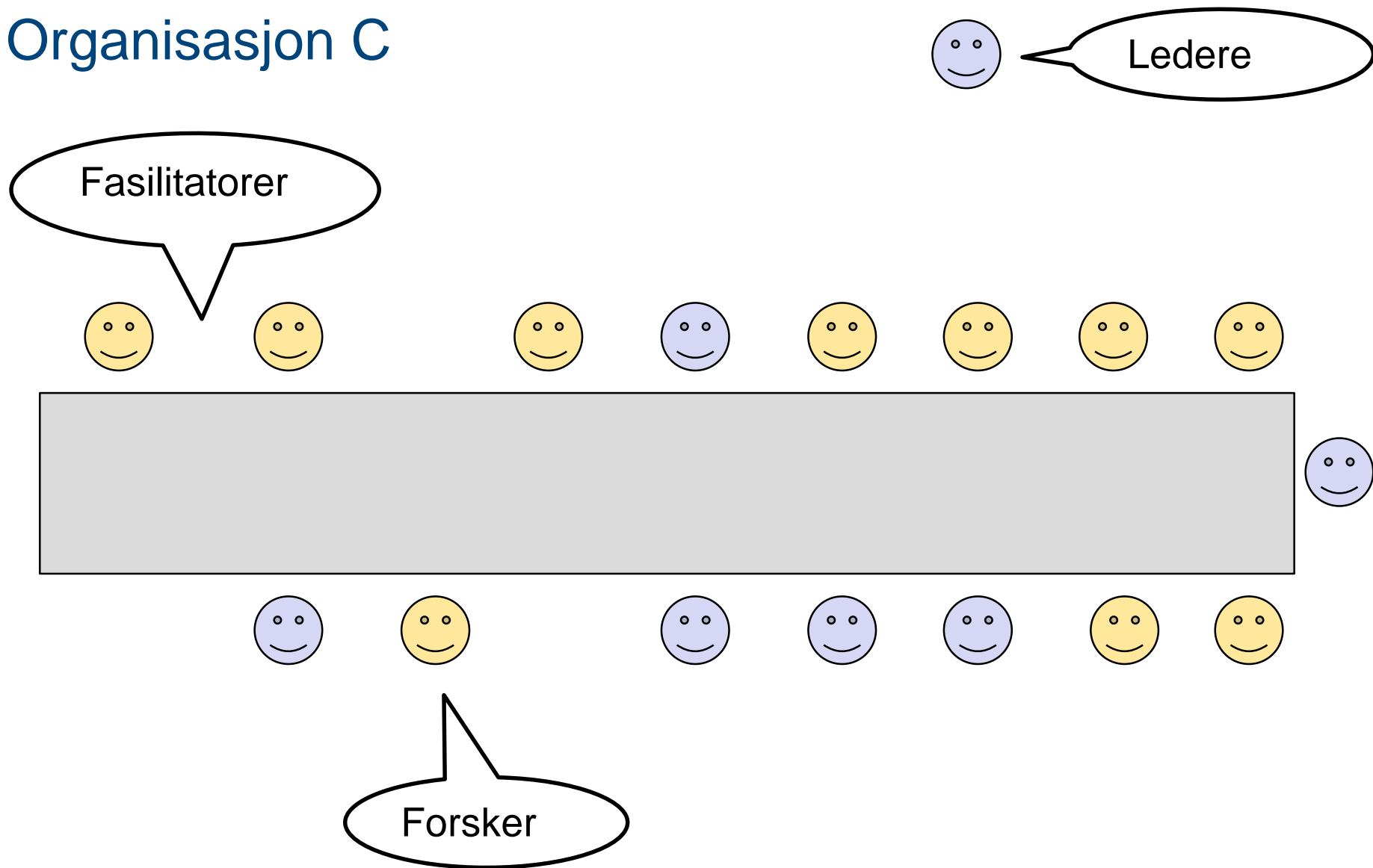


Organisasjon B

- Tre grupper, en observatør i hver gruppe.
- Beredskapsleder tilstede.

<bilder er fjernet>

Organisasjon C



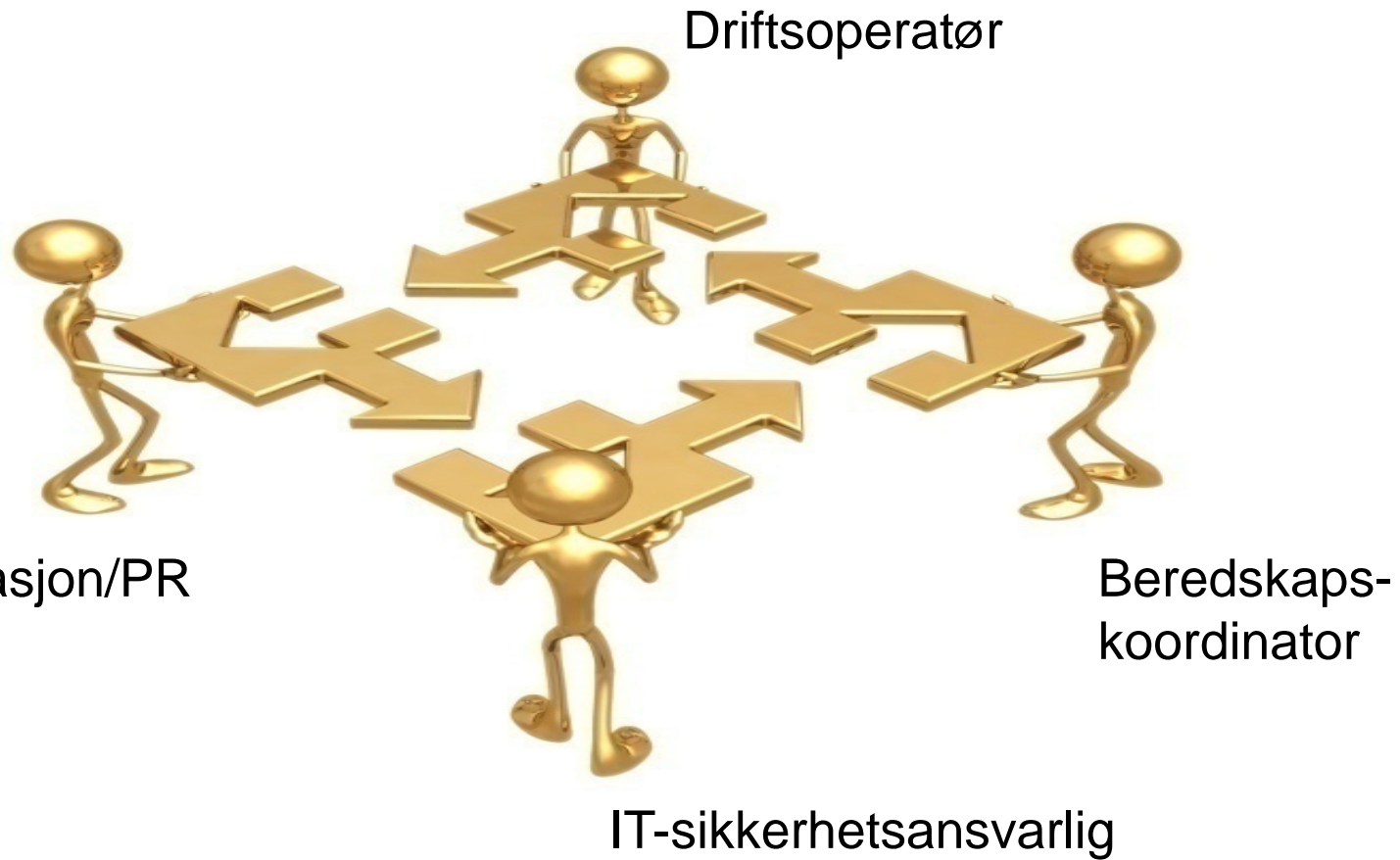
"It is crucial to us as a small organization to have a professional, large, and competent IT supplier on which we can rely on in such situations."

IT/IT security manager in a small DSO

God og effektiv hendelsehåndtering krever:

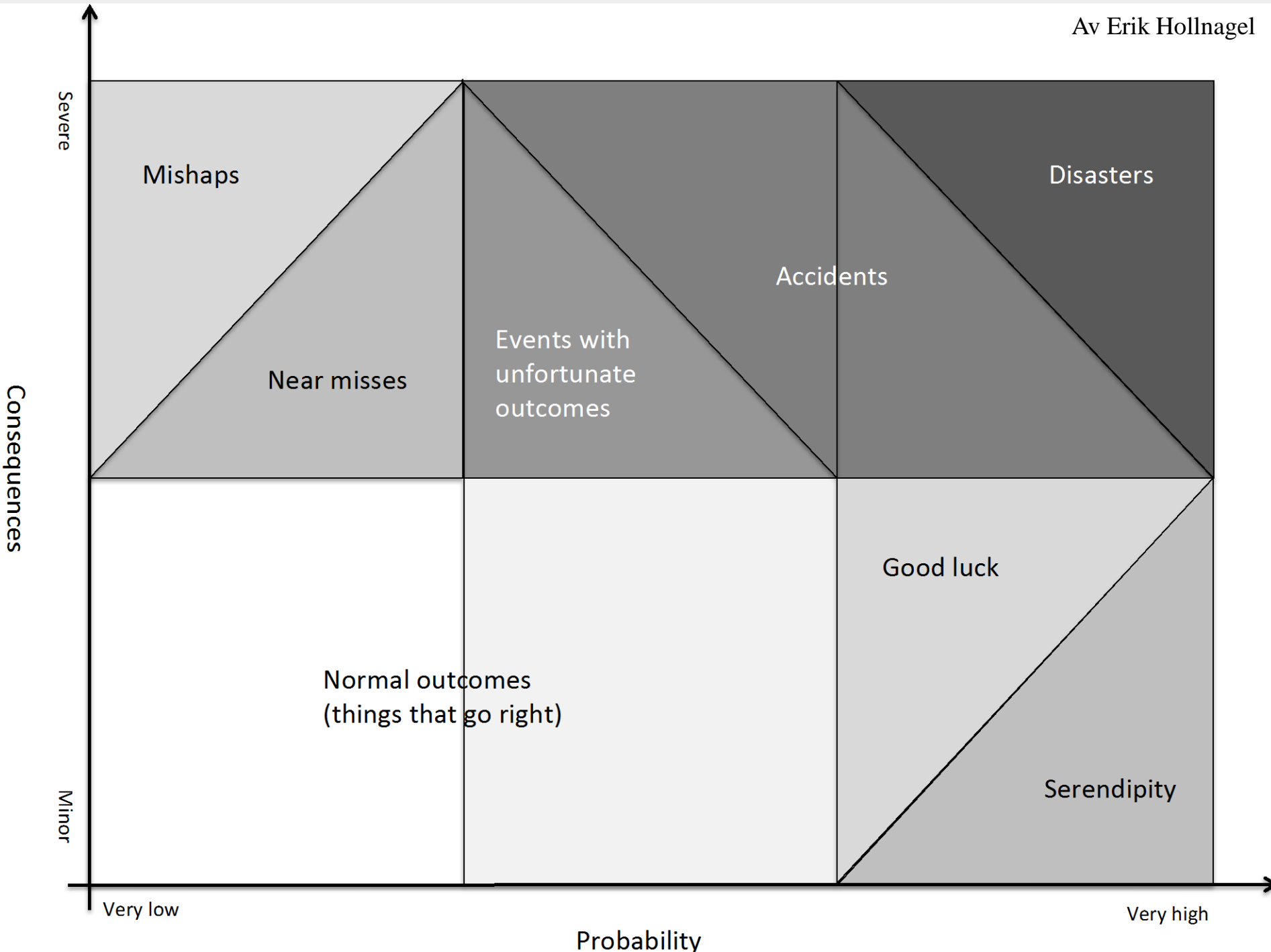
- Kryssfunksjonelle, selvstyrte team
- Evnen til å lære

Kryssfunksjonelle team



Evnen til å lære

Enkeltløkke vs. dobbelløkke

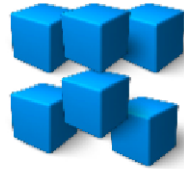


God og effektiv hendelsehåndtering krever:

- Kryssfunksjonelle, selvstyrte team
- Evnen til å lære



(a) 6 Spillerbrikker og 5 markører



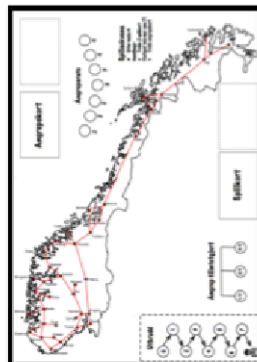
(b) 30 Angrepskuber og 5 forskningstasjoner



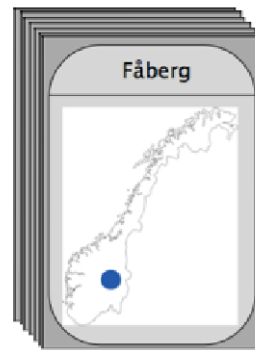
(c) 6 Rollekort



(d) 6 Angrep!!-kort



(a) Spillbrett



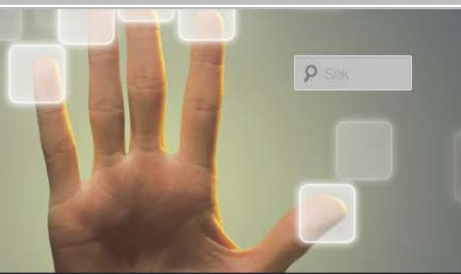
(b) 38 angrepkort med by



(c) 38 spillkort med by og fase



(d) Utvalg scenarie, spørsmål og "Visste du at.." -kort.



Måltrettede angrep mot kontrollsystemer – er kraftbransjen forberedt?

Skrevet 27. august 2014 av [Maria B. Line](#)

I dag ble det kjent at norske olje- og energibedrifter er utsatt for [tidenes mest omfattende hacker-angrep mot norske interesser](#). De faktiske konsekvensene er ennå ikke kjent, men det antydes at motivet er industrispionasje, og at angriperne har gjort endel forundersøkelser for å kunne gå mest mulig måltrett til verks.



I vår gjorde vi en intervjustudie blant norske nettselskap for å vurdere hvor godt forberedte de er på å oppdage og respondere på måltrettede angrep mot kontrollsystemene sine. Våre funn tyder på at de er godt forberedt på tradisjonelle, fysiske angrep, men IT-angrep, og spesielt avanserte måltrettede angrep, har ikke vært høyt nok oppe på agendaen deres foreløpig. [Les hele innlegget](#) →

Publisert i [Informasjonssikkerhet](#), [Konferanser](#), [Presentasjoner](#), [Prosjekter](#) | Stikkord: [kraftnettet](#), [kritisk infrastruktur](#), [måltrettede angrep](#)

Hvorfor driver vi og maser om personvern i Smart Grid?



TRANSLATE THIS PAGE (BETA)

Velg språk

Drevet av [Google](#) Oversetter

VI SKRIVER OM/ARBEIDER MED:

[accountability](#) [AMS](#) [Android](#)

[angrep](#) [ansvarlighet](#) [apps](#)

[brukskontroll](#) [cloud](#) [com-](#)

[puterworld](#) [COSTT](#) [Datalagringsdirektivet](#) [datatjenester](#) [DND](#) [SoS](#) [Facebo-](#)

[ok](#) [Google](#) [helse](#) [hendel-](#)

[seshåndtering](#) [iden-](#)

[titetshåndtering](#) [innebygd](#)

[personvern](#) [Internett](#) [ISF](#)

[konfidensialitet](#) [kraftnettet](#)

[kritisk infrastruktur](#)

[tur](#) [malware](#) [nettsky](#)

[NIK 2011](#) [ondartet](#) [kode](#) [orm](#) [over-](#)

[våking](#) [passord](#) [per-](#)

[sonvern](#) [phishing](#)

[programvare-](#)

@SINTEF_Infosec

@mariabline

infosec.sintef.no