ROS analyse for maritim digital sikkerhet

Sårbarhetsanalyse i forbindelse med strategi for maritim digital sikkerhet

September 2020

Report data

<table>
<tr><td colspan="3">Prosjekt navn:
ROS analyse for maritim digital sikkerhet</td><td rowspan="3">DNV GL AS

P.O. Box 300
1322 Høvik
Norway
+47 67 57 99 00
http://www.dnvgl.com</td></tr>
<tr><td colspan="3">Rapport tittel:
Sårbarhetsanalyse forbindelse med strategi for maritim digital sikkerhet</td></tr>
<tr><td>For:
Sjøfartsdirektoratet
Smedasundet 50A
5528 Haugesund

Kontaktperson:
Nils Haktor Bua</td><td colspan="2">Oppgave og mål:
Sårbarheter – Hvor sårbar er næringen for kjente trusler (innenfor cyberdomenet) for sektoren?

Implementeringsmodenhet – dvs. hvor godt forberedt er næringen, involvert i transport av folk og gods, til å kunne ta innover seg kjente trusler for næringen? Hvor godt forberedt er næringen, involvert i transport av folk og gods, til å kunne ta innover seg kjente trusler for næringen, forhindre hendelser og etablere en passende sikkerhetskultur? Hvor klar er en for å håndtere konsekvenser av hendelser?</td></tr>
<tr><td>Dato:
2020-09-15</td><td>Rapport nr.:
2020-0927</td><td>Revisjons nr.:
1</td></tr>
<tr><td>Project No.:
A0893962 /10179096</td><td>DNV GL dokument nr.:</td><td colspan="2">DNV GL organisasjonsenhet:
M-SA-CBC</td></tr>
<tr><td>Forberedt av:
Jarle Coll Blomhoff
Group Leader</td><td>Verifisert av:
Pål Børre Kristoffersen
Senior Principal Consultant

Are Jørgensen
Senior Principal Consultant</td><td colspan="2">Godkjent av:
Jarle Coll Blomhoff
Group Leader</td></tr>
<tr><td colspan="2">☐ OPEN. Unrestricted distribution, internal and external.
☒ INTERNAL use only. Internal DNV GL document.
☐ CONFIDENTIAL. *Distribution within DNV GL according to applicable contract.
☐ *Specify distribution: Distribution list (Default should be “DNV GL” if no other restrictions apply)
☐ SECRET. Authorized access only.</td><td colspan="2">Nøkkelord:
Maritim digital sikkerhet, Risiko og sårbarheter, Cyber security,</td></tr>
<tr><td colspan="4">Referanse til deler av denne rapporten som kan lede til mistolkning er ikke tillatt</td></tr>
</table>

Innholdsoversikt

Sammendrag

Oppdrag

- **Sjøfartsdirektoratet har fått i oppdrag** fra Nærings- og fiskeridepartementet å 'Lede arbeidet med utarbeidelse av en **overordnet strategi for maritim digital sikkerhet**'.
- I den sammenhengen har **DNV GL utført en risiko-, sårbarhet- og modenhetssanalyse** med fokus på skipsdrift, og hvordan IKT sikkerhetstrusler påvirker bransjen basert på vår kompetanse og spørreundersøkelse mot skipseiere i Norge.

Risiko & modenhet

- **IKT risiko ift. sikker skipsdrift er vurdert ulik for IT systemer og OT (kontroll) systemer. For IT er risikoen lav til middels** siden konsekvensen for skipsdrift er lav, modenheten for tiltak er høy – selv om sannsynlighet for en hendelse er relativt høy. For **OT (kontroll) systemer er risikoen vurdert til middels til høy** siden konsekvensen for skipsdrift kan være høy og modenheten for tiltak er lav, selv om sannsynlighet for en hendelse er relativt lav. I tillegg forventer vi en utvikling med mer fjerntilkobling, integrering og digitalisering av OT systemer.
- IT **systemer i bruk i den maritime sektoren skiller seg lite fra IT systemer i andre bransjer**, og er bygget på forholdsvis moden teknologi når det kommer til IKT sikkerhet. DNV GL anbefaler derfor sjøfartsdirektoratet og **fokusere arbeidet på brosystemer og kontrollsystemer**.

Anbefaling

- De **kritiske systemene for å opprettholde sikker skipsdrift bør prioriteres**. Risiko bør vurderes for hver enkelt installasjon siden det er store ulikheter i kontrollsystemene og lokal- og fjerntilgang for disse systemene. **Viktige tiltak er skallsikring/segregering av kritiske systemer**, system barrierer og hendelseshåndtering.
- Den maritime bransjen i Norge er **moden når det gjelder IT systemer** og håndtering av disse risikoene, men **for OT (kontroll og bro systemer) gjenstår det fortsatt et stykke arbeid** som bør støttes av Sjøfartsdirektoratet.

Maritim Digital Sikkerhet

Prosjektbeskrivelse og industritrender

Prosjektbeskrivelse og rammer for analysen

Kundebehov

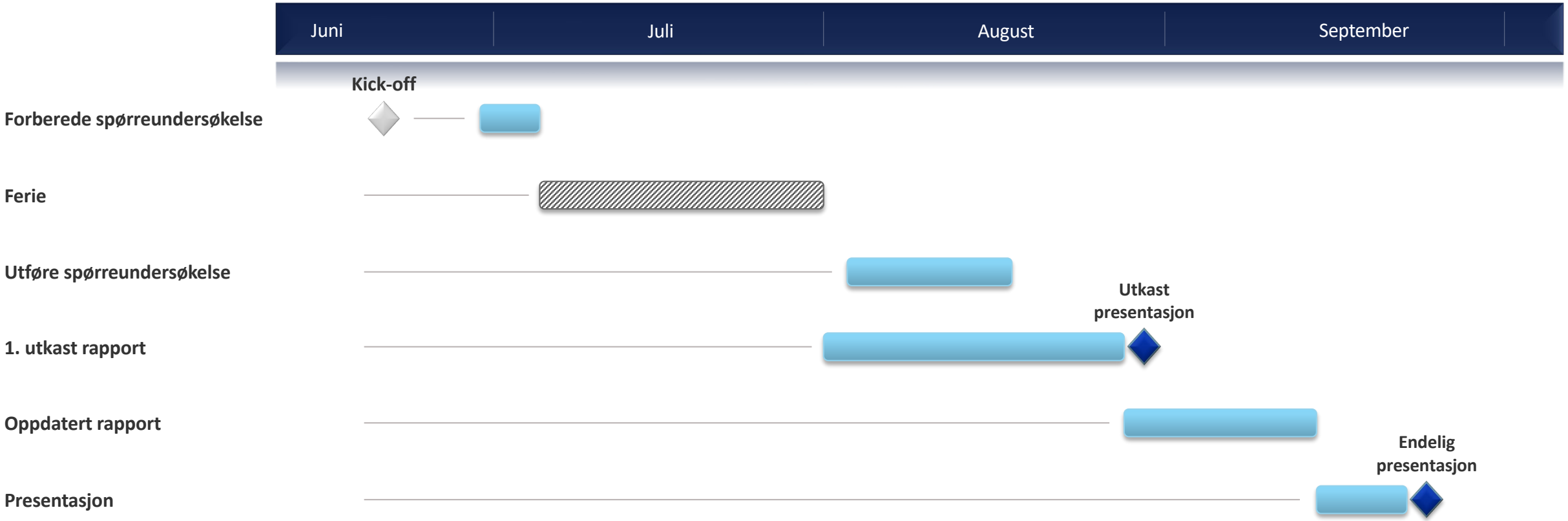
- Sjøfartsdirektoratet har fått i oppdrag fra Nærings- og fiskeridepartementet å '***Lede arbeidet med utarbeidelse av en overordnet strategi for maritim digital sikkerhet***'.
- Som grunnlag for å komme med tiltak og retning i strategien ønsker direktoratet å ha et best mulig ***grunnlag for dagens status gitt sårbarheter og trusler i maritim næring***. Denne sårbarhetsanalysen vil ***fokusere på skipsoperasjon og drift, og vurdere grensesnitt i operasjon mot leverandører***. Andre deler av maritim næring som f.eks. ***skipsbygging og havnedrift vil ikke være i fokus*** for denne analysen.

Oppdragsbeskrivelse

1. ***Sårbarheter*** – Hvor sårbar er næringen for kjente trusler (innenfor cyberdomenet)?

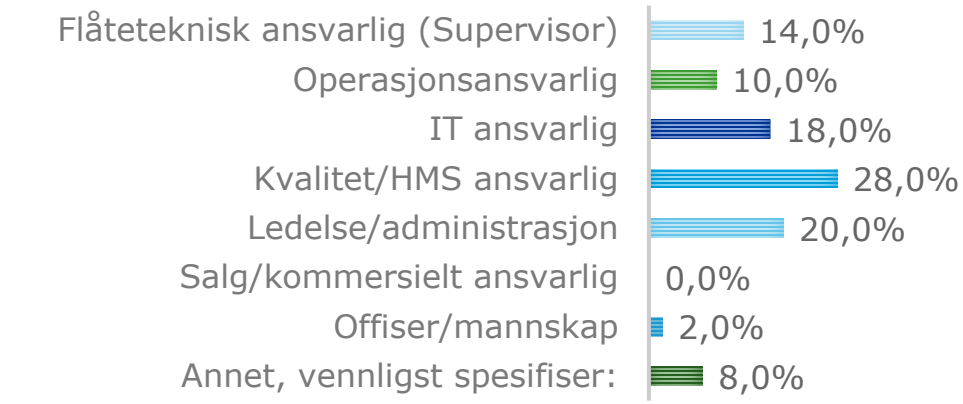
2. ***Implementeringsmodenhet*** – dvs. hvor godt forberedt er næringen, involvert i transport av folk og gods, til å kunne ta innover seg kjente trusler for næringen? Hvor godt forberedt er næringen, involvert i transport av folk og gods, til å kunne ta innover seg kjente trusler for næringen, forhindre hendelser og etablere en passende sikkerhetskultur? Hvor klar er en for å håndtere konsekvenser av hendelser?

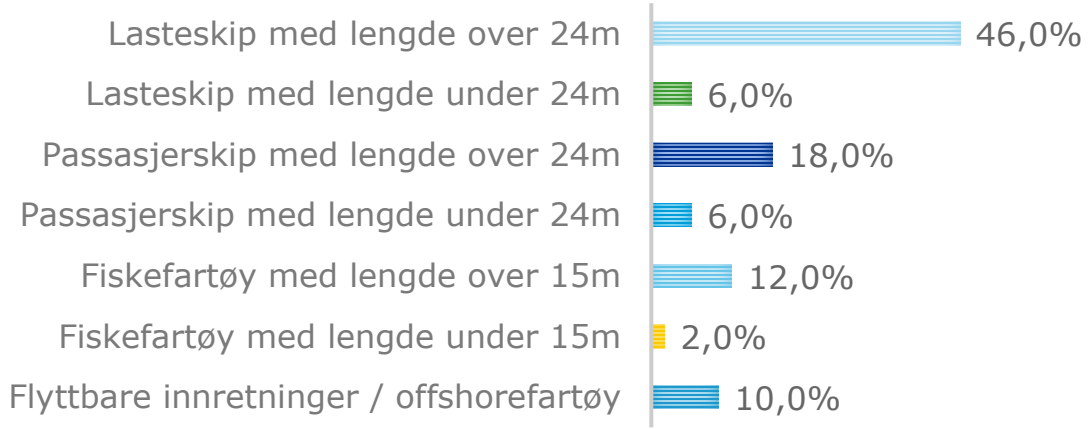
Prosjektaktiviteter og fremdrift



En spørreundersøkelse til maritim industri i Norge ble utført i forbindelse med risiko- og sårbarhetsanalysen

- **Spørreundersøkelsen ble utarbeidet av DNV GL på vegne av Sjøfartdirektoratet** som var avsender/oppdragsgiver for spørreundersøkelsen.
- Undersøkelsen ble utført **anonymt** med **QuestBack** som verktøy.
- Svar ble samlet inn **fra medlemmer av fire relevante sjøfartsforbund** i Norge: Norges rederiforbund, Hurtigbåtforbundet, Fiskebåt, Kystrederiene og NHO Sjøfart.
- **51 svar er mottatt** fra ulike selskaper.





Maritim digital sikkerhet er omfattende område med viktig samfunnsbetydning - Fokus for denne risiko- og sårbarhetsanalysen (ROS) er sikker fartøydrift

- ***Maritim digital sikkerhet påvirker hele den maritime industrien i Norge*** med aktører som eiere, operatører, leverandører, verft, myndigheter, forsikring og finans i tillegg til industri og private som er avhengig av bransjen som transport medium nasjonalt og internasjonalt.
- Denne begrensede ROS analysen ser på digital risiko og sårbarheter for ***selve skipsdriften, med grensesnitt mot leverandører i driftsfasen***.
- **Terrorhendelser/angrep med bruk av infrastruktur** manipulasjon utenfor skipet **er ikke vurdert**, f.eks. **radiosystemer**, **GPS/AIS «spoofing»/«jamming».**
- **Selskapsrisiko** mot forsikring og finans, **nybyggrisiko** mot verft og leverandører, og **logistiskrisiko** i forhold til havner og andre aktører er også viktige elementer innen maritim digital sikkerhet, men er **ikke dekket i denne analysen**.

Digital sikkerhetsrisiko grunnes både uønskede utilsiktede og tilsiktede hendelser

Digital risiko

Utilsiktede hendelser

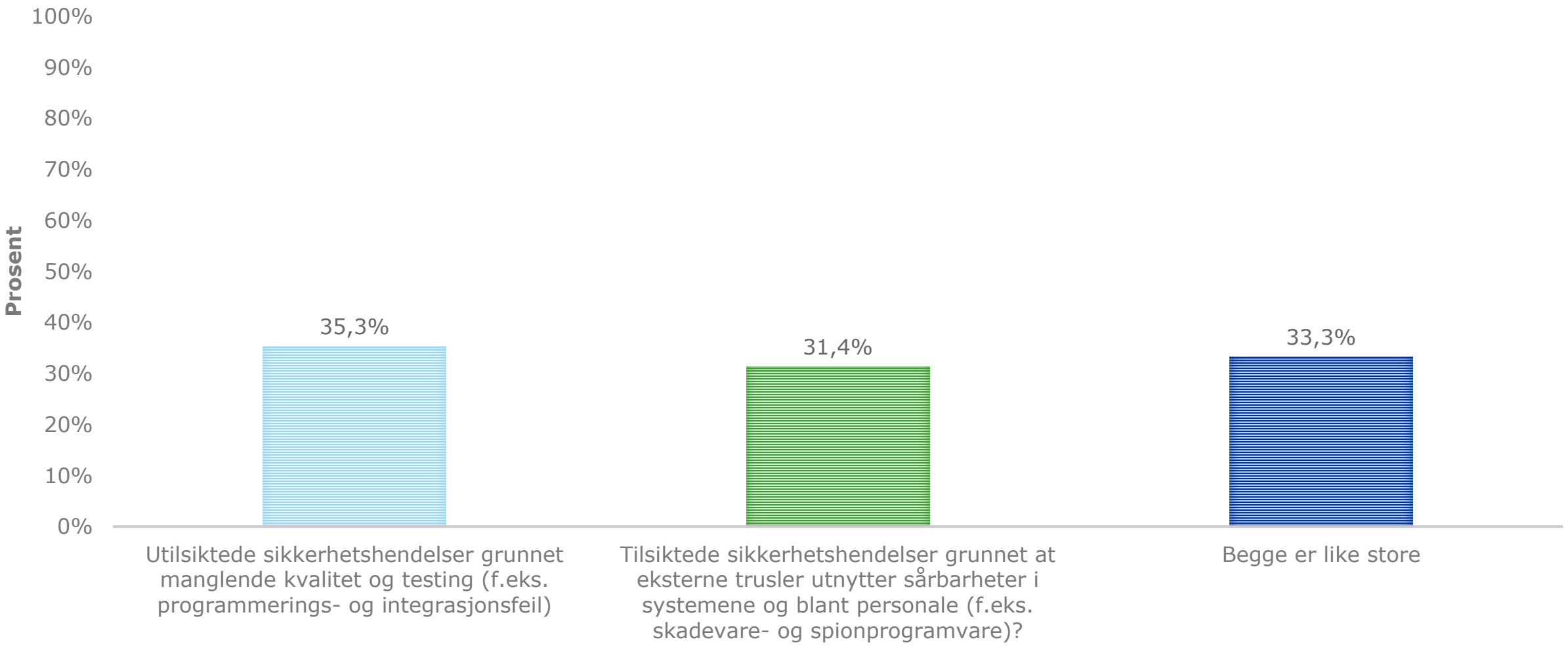
- ... viser til hendelser grunnet bl.a. feil i programvare og maskinvare og uhell knyttet til vedlikehold og operasjon.
- … og kan sikres gjennom en strukturert prosess med design, utvikling, testing, distribusjon og drift. Det bør håndteres med gode prosedyrer, tekniske løsninger og kompetent personell.

Fokus for ROS analysen

Tilsiktede hendelser

- … viser til ondsinnede hendelser som utnytter sårbarheter i programvare og maskinvare eller menneskelige svakheter. Eksempler er digitale angrep og sosial manipulasjon.
- … og bør sikres ved tekniske sikkerhetstiltak, organisatoriske prosesser og trening av personell.

Hva er etter i din mening den største trusselen i forbindelse med softwarebaserte systemer om bord?



"Besvarelsene fra spørreundersøkelsen indikerer en god forståelse for de ulike typene IKT sikkerhetshendelsene"

Trender som driver det digitale sikkerhetsbildet for maritim skipsdrift

Digitalisering

- ***Skipsteknologi endres*** *fra mekanikk/elektronikk og proprietær teknologi til hyllevare/standardisert program- og maskinvare*
- ***Økt kompleksitet*** *med mer programvare, automatisering, integrasjon og fjerntilgang*
- ***Digital sikkerhet er et kritisk element*** *som må være på plass for å sikkert kunne ta i bruk og realisere de fordelen digitale verktøy kan gi*

Hendelser

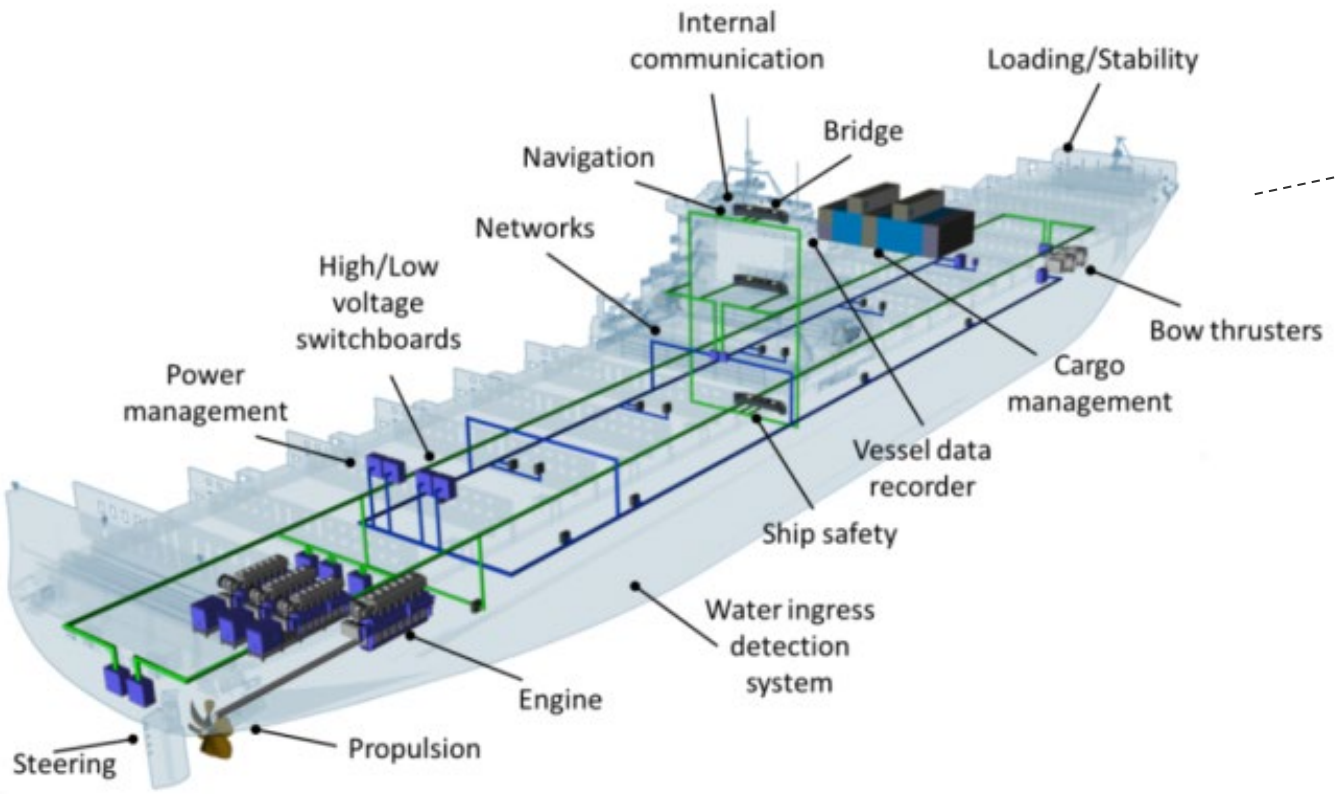
- ***Antall digitale sikkerhetshendelser øker*** *sterkt med økningen i digital bruk i industrien*
- ***Både IT*** *(informasjonsteknologi) og* ***OT*** *(operasjonellteknologi) rammet, men mest innen IT*
- ***Begrenset transparens*** *og erfaringsutveksling indikerer store mørketall*

Regulering

- ***Nye nasjonale og internasjonale lover og regler innføres*** *som f.eks. IMO cyber risk resolusjonen,* MSC.428(98), EU GDPR og NIS-direktivet.
- ***Finansiell påvirkning*** *via kommersielle krav fra befrakter (TMSA), operatører, finans og forsikring*

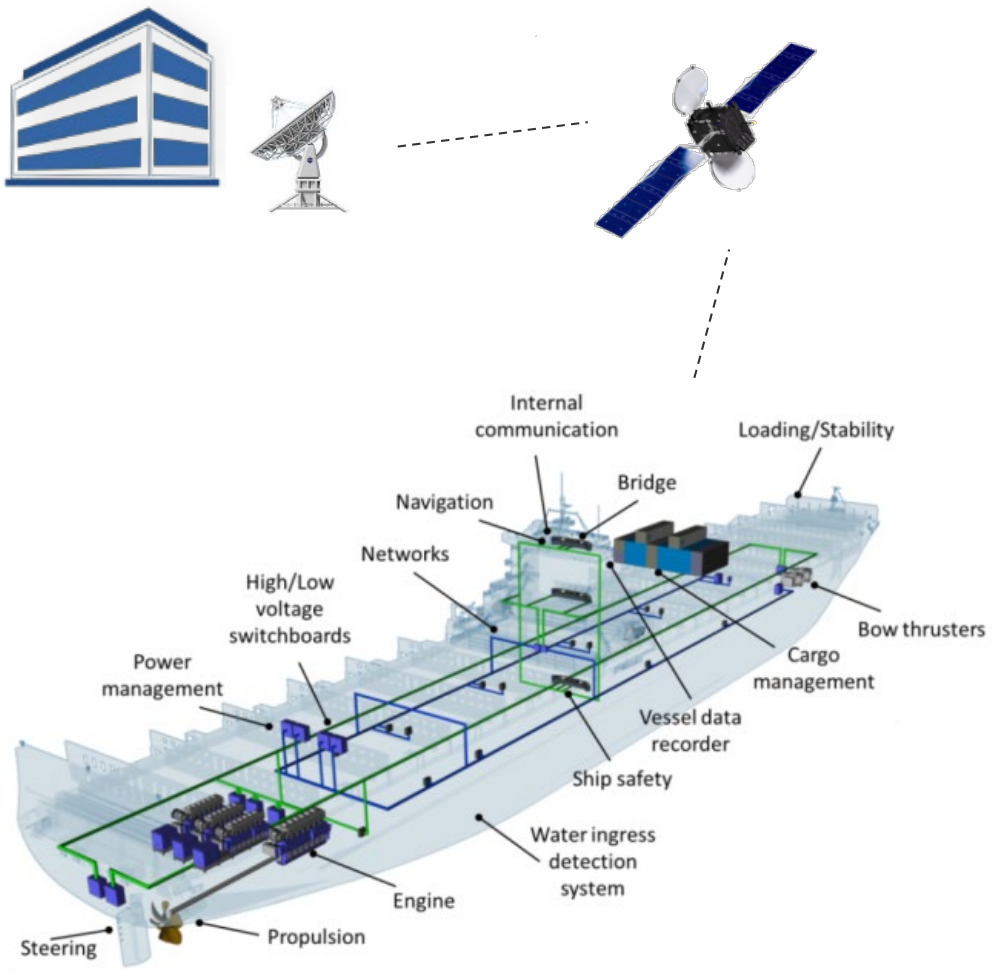
Digitale systemer er utbredt om bord i et moderne kommersielt fartøy

Om bord



Land organisasjon

Digitale systemer om bord kan inndeles i informasjon- og operasjonsteknologi



Informasjonsteknologi (IT) på land og ombord

- IT-nettverk
- Administrasjon, E-post, finans, administrasjon, brukerkontoer, mannskapslister, etc.
- Vedlikeholds-data
- Lagerbeholdning og innkjøp av deler og materiell
- Elektroniske dokumenter og formularer
- Kontrakter, Lastinformasjon,
- …

Operasjonsteknologi (OT) ombord

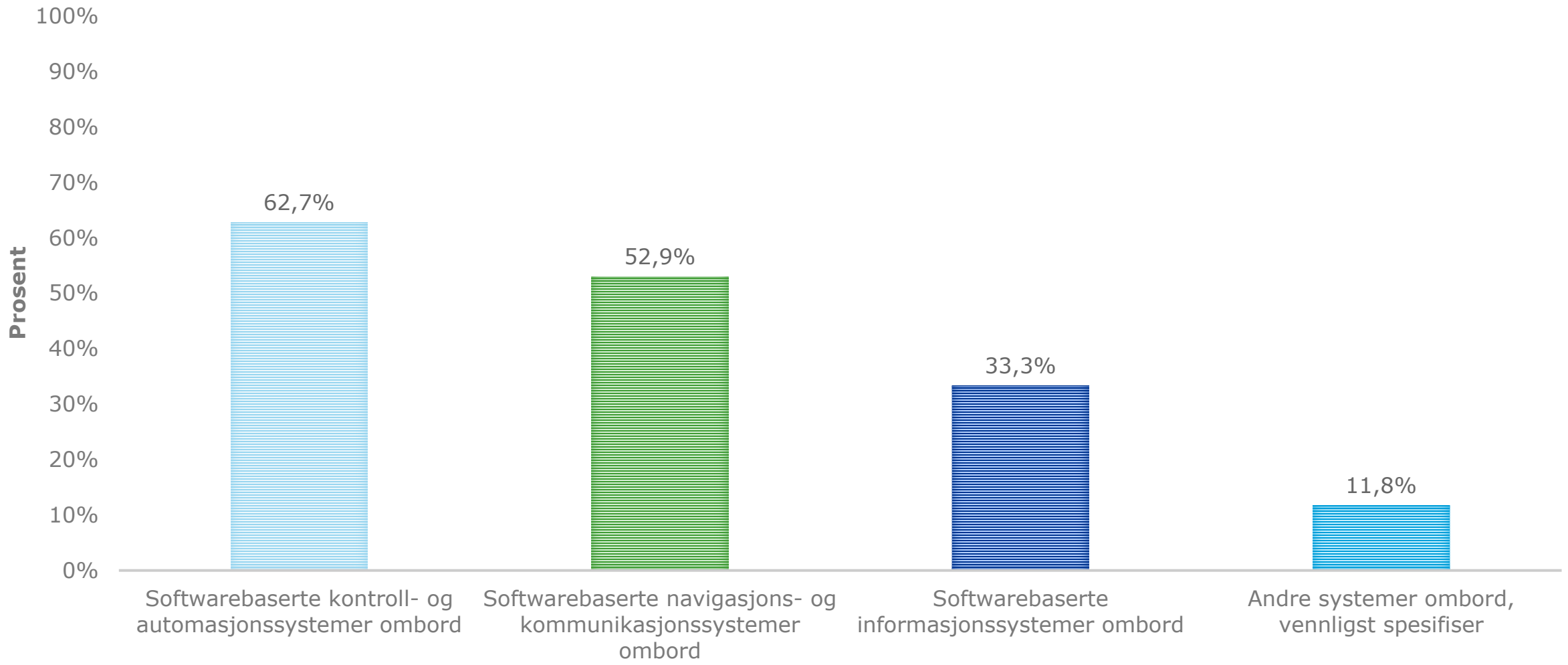
Kontrollere, SCADA nett, sensorer, styringssystemer, navigasjonsdata

- Fremdrift, styring og energiforsyning
- Branndeteksjon og slukking
- Ballast systemer
- Navigasjon og kommunikasjon
- Produksjonssystemer (boring, kraner, trål, …)
- Støttesystemer
- …

Maritim Digital Sikkerhet

Risiko, trusler og sårbarheter

Hvilke systemer om bord anser du for å være mest sårbare for digitale sikkerhetshendelser?



"Det er en felles forståelse i industrien for at kontroll systemene er mest sårbare ifm IKT sikkerhetshendelser"

Risiko analysen bygger på anerkjent metoder for vurdering av sannsynlighet og konsekvens – med fokus på sikkerhet som mål

RISIKO = Konsekvens av gitt hendelse x Sannsynlighet for at hendelsen inntreffer

En gitt hendelse med tilhørende konsekvens kan påvirke ulike mål definert av selskapet f.eks.:

Sikkerhet	Finansiell	Omdømme og juridisk	Miljø
Sikkerhet *kan f.eks. beskrive mulige konsekvenser som påvirker skipets og mannskapets sikkerhet*	***Finansiell*** *mål beskriver mulige konsekvenser som kan påvirke selskapets økonomi*	***Omdømme eller juridisk*** *mål beskriver mulige konsekvenser som kan påvirke selskapets rykte og samsvar med lover og regler*	***Miljø*** *mål beskriver mulige konsekvenser som kan påvirke miljøet*
=> Sikkerhet kan vurderes i forhold til typisk skipsdrift, men en skips-spesifikk vurdering må også utføres	*=> Avhenger av selskapets forretningsplan, og må vurderes av hver enkelt aktør*	*=> Avhenger sterkt av selskapets historie, struktur og relasjoner*	*=> Avhenger sterkt av selskapets last, operasjons-område og lokale lover og regler*

Fokus

IT-systemer på land og ombord baserer seg på moderne digital sikkerhetsteknologi og skiller seg lite fra andre industrier

Digital sikkerhets modenhet

- IT systemer for landorganisasjonen er standardiserte og **skiller seg lite fra andre typer selskaper.**
- IT systemer ombord **skiller seg teknisk sett lite fra andre kontorbaserte IT-systemer.**
- Disse systemene er **ofte under ansvarsområdet til selskapets egen IT-avdeling.**
- **Etablerte prosedyrer og teknologier er modne**, tilgjengelige og tatt i bruk i næringen.
- Modenhet og **profesjonalitet antas å øke med størrelsen** på selskapet.

Overordnet risikovurdering

- IT systemene er basert på **hyllevare teknologi**, både for nettverkskomponenter, maskinvare og programvare.
- Systemene er derfor **mer sårbare for skadevare** som er rettet mot de mest brukte standardsystemene.
- I tillegg har IT systemene **omfattende grensesnitt både internt på skipet og mot internett.**
- Sannsynligheten for angrep er derfor forholdsvis høy, men systemene ikke er kritisk for skipsdriften.
- Fordi modenheten for IT-styring er høyere, anser vi at **konsekvensen og tilhørende risiko for skipssikkerheten er lav til middels**.
- **Konsekvenser knyttet til økonomi, miljø, omdømme og overholdelse av lover og regler kan være omfattende**, men er ikke behandlet i denne analysen.

Industrispesifikke behov

- Selv om vi anbefaler den maritime industrien i Norge å følge overordnede tiltak for IT-systemer fra Nasjonal strategi for digital sikkerhet, er det noen spesielle hensyn som bør tas.
  - Drift i kortere eller lengre **perioder med begrenset båndbredde** for å kunne oppdatere systemer.
  - **Stor variasjon i IKT-sikkerhetskompetanse hos mannskap**, og ofte mannskap med midlertidig ansettelse om bord.
  - **IT-systemene er ofte en inngangsport til bro og kontrollsystemer ombord**, dette grensesnittet må derfor sikres spesielt.

➢ Lite behov for industrispesifikke retningslinjer for IT-systemene om bord og på kontoret

OT-systemer ombord baserer seg ofte på eldre teknologi, har mangelfulle sikkerhetsbarrierer, stor konsekvens ved hendelser og blir mer og mer digitale

Digital sikkerhets modenhet

- **OT-systemer ombord er ofte skreddersydde systemer**, og det er stor forskjell i teknologi og praksis mellom ulike skip.
- **IKT-sikkerhetsansvar for disse systemene er ofte uavklart**, og det håndteres vanligvis av en eller flere personer fra leverandører, flåteteknisk avdeling og/eller IT-avdeling.
- Mange selskaper **mangler moderne prosedyrer og teknologi for IKT-sikkerhet** for OT-systemer.
- En viktig faktor for å håndtere IKT-sikkerhet for OT-systemer er **samarbeid mellom IT- og flåte-ressurser.**

Overordnet risikovurdering

- OT-systemene har **tradisjonelt vært basert på proprietære teknologier, men bruker nå mer og mer hyllevare-teknologi,** for å spare kostnader og utviklingstid.
- Systemene blir derfor etterhvert **mer sårbare for skadevare** som er rettet mot standardsystemer.
- OT-systemer har ofte vært **designet for å driftes frittstående, men blir nå mer og mer integrert og tilkoblet** både internt på skipet og ekstern mot landbaserte installasjoner.
- Sannsynlighet er ennå ansett som lav, men siden systemene er kritisk for skipsdriften og siden IKT-sikkerhet er mindre modent, anser vi **konsekvensen og tilhørende risiko for skipssikkerheten som middels til høy**

Industrispesifikke behov

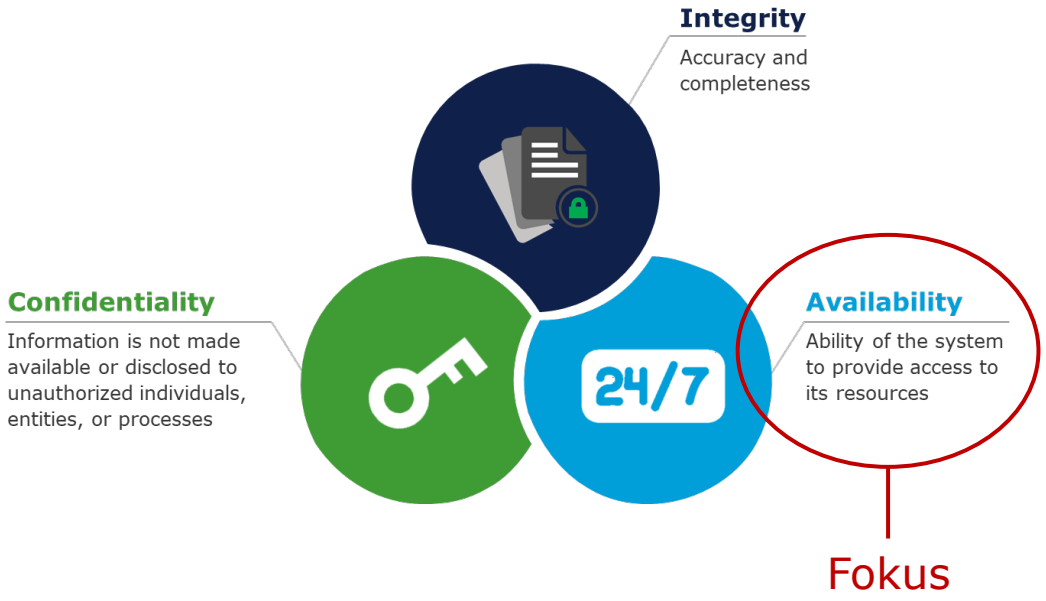
- Maritim industri er en global industri som i stor grad **følger definerte lover og regler**, og har i motsetning til olje og gass industrien **mindre fokus på tiltak fra spesifikke risikovurderinger.**
- Det er derfor **behov for industrispesifikke veiledninger.**
- Disse bør være **i tråd med internasjonale lover og regler** grunnet industriens internasjonale karakter og konkurransesituasjon.
- **Klare retningslinjer og krav vil være en fordel for næringen fordi den har et stort antall leverandører** som tilbyr systemer til skip som ofte bygges i andre regioner enn der de skal driftes.

➢ Behov for industrispesifikke retningslinjer for IKT-sikkerhet for OT-systemene om bord

IKT risikoanalyser skiller seg fra tradisjonell risikoanalyse for sannsynlighet (tilgang) og konsekvens (konfidensialitet, integritet og tilgjengelighet)

RISIKO = Konsekvens av gitt hendelse x Sannsynlighet for at hendelsen inntreffer

- *IKT risikovurdering ser ofte på andre konsekvenser enn tradisjonell risikovurdering, typisk konfidensialitet, integritet og tilgjengelighet. For OT systemer er tilgjengelighet ofte hovedmålet*



- *Tilgangsvurdering erstatter tradisjonell sannsynlighet pga. manglende data/statistikk*

Fjern tilgang	Fysisk tilgang	Integrert med andre systemer	Krever software oppdatering	Tilgangs-vurdering
X	-	-	-	Middels
X	-	-	X	Høy
X	-	X	Ingen effekt på tilgang	Høy
X	X			Høy
-	-	X		Middels
-	X	-		Middels
-	X	X		Middels
X	X	X		Høy
-	-	-	X	Middels
-	-	-	-	Lav

Eksempel for tilgangsvurdering (sannsynlighet) DNVGL-RP-0496

Konsekvensene av hendelser kan vurderes ut ifra hvor viktige systemene er for å opprettholde sikker drift av skipet

Høy

Systemer som må være i kontinuerlig drift **for å beholde skipets manøvreringsevne** er definert som de **kritiske systemene med høy konsekvens for skipets sikkerhet**

Middels

Systemer som ikke må være i kontinuerlig drift, men som kan **forårsake en kritisk situasjon i gitte scenarier** er vurdert som **systemer med middels konsekvens for skipets sikkerhet**

Lav

Systemer som kun har en **støttefunksjon eller informasjonsrolle i skipsdriften** er vurdert som systemer med **lav konsekvens for skipets sikkerhet**

Generell konsekvensvurdering av typiske skipssystemer (1/3)

System	Konsekvens	Kommentar*
Fremdriftssystemer	Høy	Fremdriftsmotorer, propellvridning, hastighet, thruster'e, pod'er …
Styringssystemer	Høy	Ror, azimuth thrustere, hydraulikksystemer, …
Vanntett integritet	Høy	Luker, skalldører og innvendig vanntette dører
Kraftproduksjon	Høy	Kraftproduksjon for styring og fremdrift
Nødvendige støttesystemer	Høy	Pumper, vifter, kjøling, osv. som er kritisk for å opprettholde de viktigste systemene
Sikkerhetssystemer	Høy	Systemer som sørger for «fail-safe» funksjon for kritiske systemer må alltid være i drift
Alarm- og automasjonssystemer	Middels	Alarm- og automasjonssystemer er sentralt for drift av kompliserte skip med begrenset bemanning, men det er forventet at skipet kan seile sikkert i en begrenset periode uten
Branndeteksjon og slukkesystemer	Middels	Dersom en nødsituasjon skulle oppstå med brann, er disse systemene kritiske
Ballaststyring	Middels	Ballastsystemer kan endre manøvreringsevnen til et skip, og kan være kritisk i visse værsituasjoner
Hjelpepropeller	Middels	Baugpropeller og lignende systemer kan være kritiske i spesielle situasjon, f.eks. fortøyning
Navigasjonssystemer	Middels	Navigasjonssystemer er viktig for mannskap ifm sikker manøvrering, men de er også trenet på å drift skipet uten disse (Radar, ECDIS, kompass, plotter, AIS, GPS, …)
Kommunikasjonssystemer	Middels	Kommunikasjonssystemer er viktige for mannskapet for å håndtere trafikksituasjonen og nødsituasjoner (nødpeilere, høyttalersystemer, alarmsystemer, satellittkommunikasjon, …)

Konsekvensvurderingen er ment som et innspill til risiko-, konsekvens- og sårbarhetsanalysen for et skip, men erstatter ikke skips- og operasjonsspesifikke vurderinger, eller vurdering mot andre mål (økonomi, osv.)

*Selv om manuell operasjon skal være mulig, vil de likevel kunne oppstå kritiske situasjoner når systemene går ned

Generell konsekvensvurdering av typiske skipssystemer (2/3)

System	Konsekvens	Kommentar*
Lastrelaterte systemer	Middels	Laste- og lossesystemer, og lastestyringssystemer kan være kritiske for skip og mannskap, og disse systemene kan også vurderes til Høy konsekvens. Kraner, ramper, reefer, boil off gas, inert gas, VOC systemer er eksempler på viktige slike systemer
Fiskerisystemer	Middels	Fiskerisystemer er kritiske for fiskebåtens evne til å utføre sin oppgave, og vil i enkelte situasjoner vurderes høy siden den kan ha kritisk påvirkning på både skip og mannskap
Evakuerings- og sikkerhetssystemer	Middels	I en nødsituasjon er det kritisk at disse systemene opererer som planlagt for å redde liv til mannskap og passasjerer
Forankringssystemer	Middels	I situasjoner med dårlig vær og tett trafikk kan disse systemene påvirke skipets sikkerhet
Lyssystemer	Middels	Lys- og lydsystemer kan være kritiske ifm navigering i mørket og dårlig vær
Olje – og gass driftssystemer	Middels	Avhengig av skip, oppdrag og operasjon vil nok offshore skip ofte vurdere disse systemene med høy konsekvens
Varme-, kjøling- og ventilasjonssystemer	Lav	HVAC systemer sørger for komfortable arbeidsbetingelser om bord, men er i de fleste tilfeller ikke kritisk for skipsdriften
Miljø- og utslippssystemer	Lav	Feil ved miljø- og utslippssystemer kan medføre store miljøpåvirkninger og rettslige- og økonomiske konsekvenser, men er i de fleste tilfeller ikke kritisk for skipsdriften (behandlingssystemer for ballastvann, scrubber'e, …)

Konsekvensvurderingen er ment som et innspill til risiko-, konsekvens- og sårbarhetsanalysen for et skip, men erstatter ikke skips- og operasjonsspesifikke vurderinger, eller vurdering mot andre mål (økonomi, osv.)

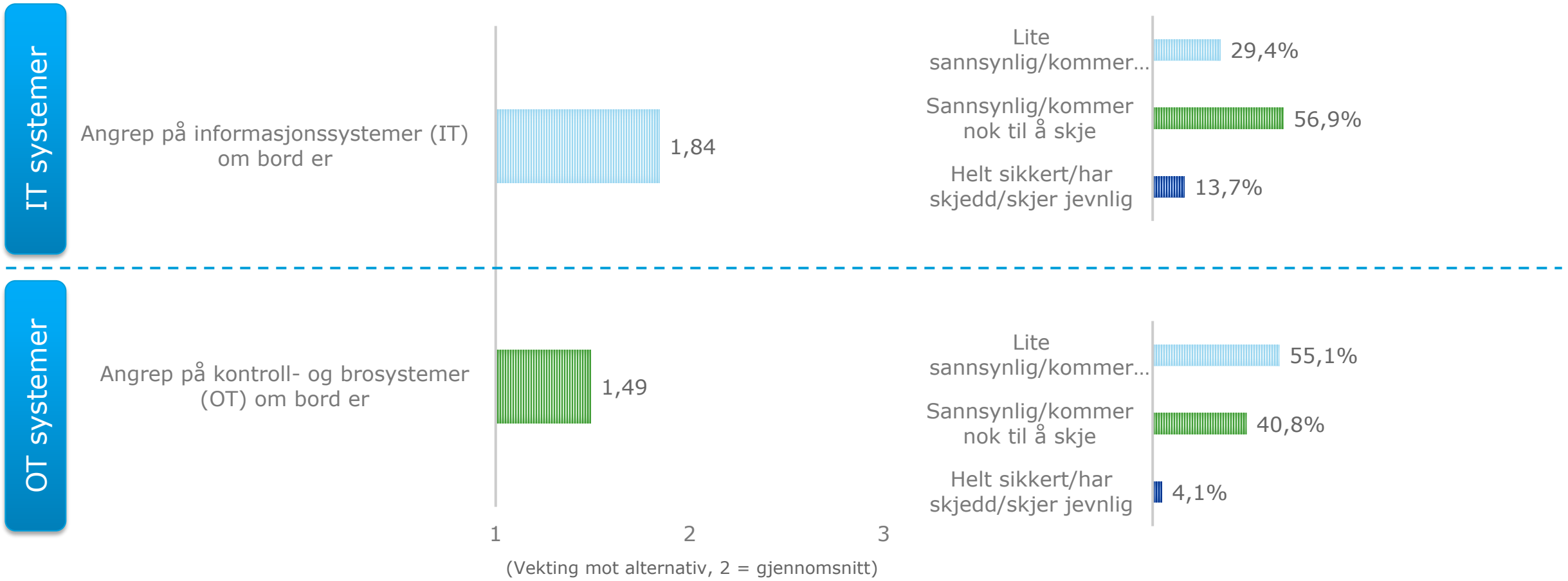
*Selv om manuell operasjon skal være mulig, vil de likevel kunne oppstå kritiske situasjoner når systemene går ned

Generell konsekvensvurdering av typiske skipssystemer (3/3)

System	Konsekvens	Kommentar
Energi/miljøstyringssystemer	Lav	Slike systemer kan effektivisere driften og miljø påvirkning, men er i de fleste tilfeller ikke kritisk for skipsdriften
Passasjerinformasjonssystemer	Lav	Passasjerinformasjonssystemer er viktig både med tanke på private data og lover og regler, men er i de fleste tilfeller ikke kritisk for skipsdriften
Lastinformasjonssystemer	Lav	Lastinformasjonssystemer er viktig for å optimalisere logistikken for det som fraktes, men er i de fleste tilfeller ikke kritisk for skipsdriften
Underholdningssystemer	Lav	Underholdningssystemer er viktig for å ha fornøyde passasjerer og kunder, men er i de fleste tilfeller ikke kritisk for skipsdriften
Betalingssystemer	Lav	Betalingssystemer om bord kan ha stor økonomisk og omdømmepåvirkning, men er i de fleste tilfeller ikke kritisk for skipsdriften

Konsekvensvurderingen er ment som et innspill til risiko-, konsekvens- og sårbarhetsanalysen for et skip, men erstatter ikke skips- og operasjonsspesifikke vurderinger, eller vurdering mot andre mål (økonomi, osv.)

Hvor sannsynlig anser du at et angrep på kontroll og informasjonssystemer ombord er?



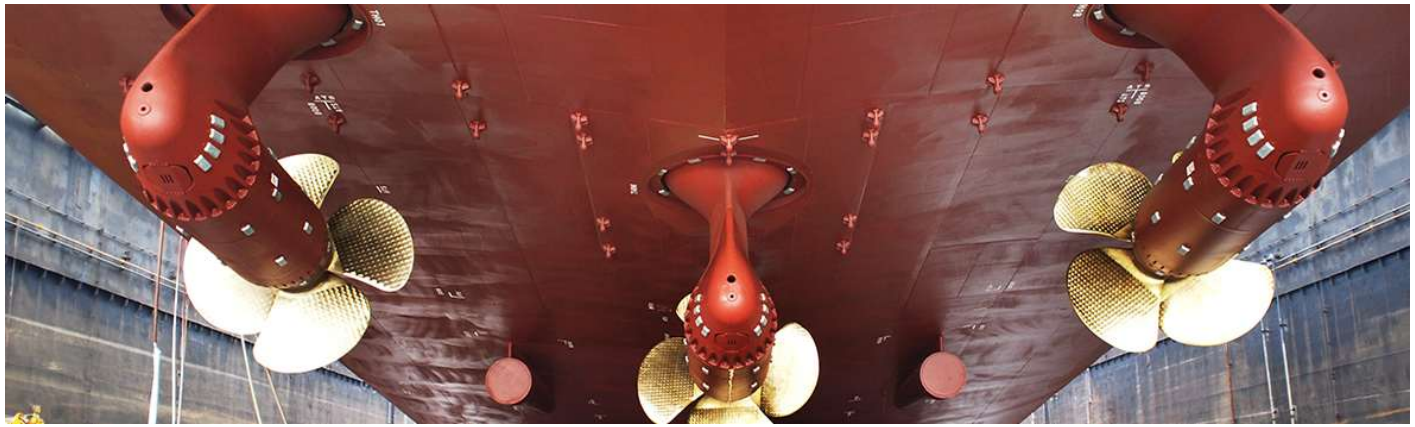
"Sannsynlighet for angrep på OT systemer rangeres tydelig lavere enn sannsynlighet for angrep på IT systemer"

Eksempel: risikovurdering av en spesifikk installasjon

IR – Initial risiko

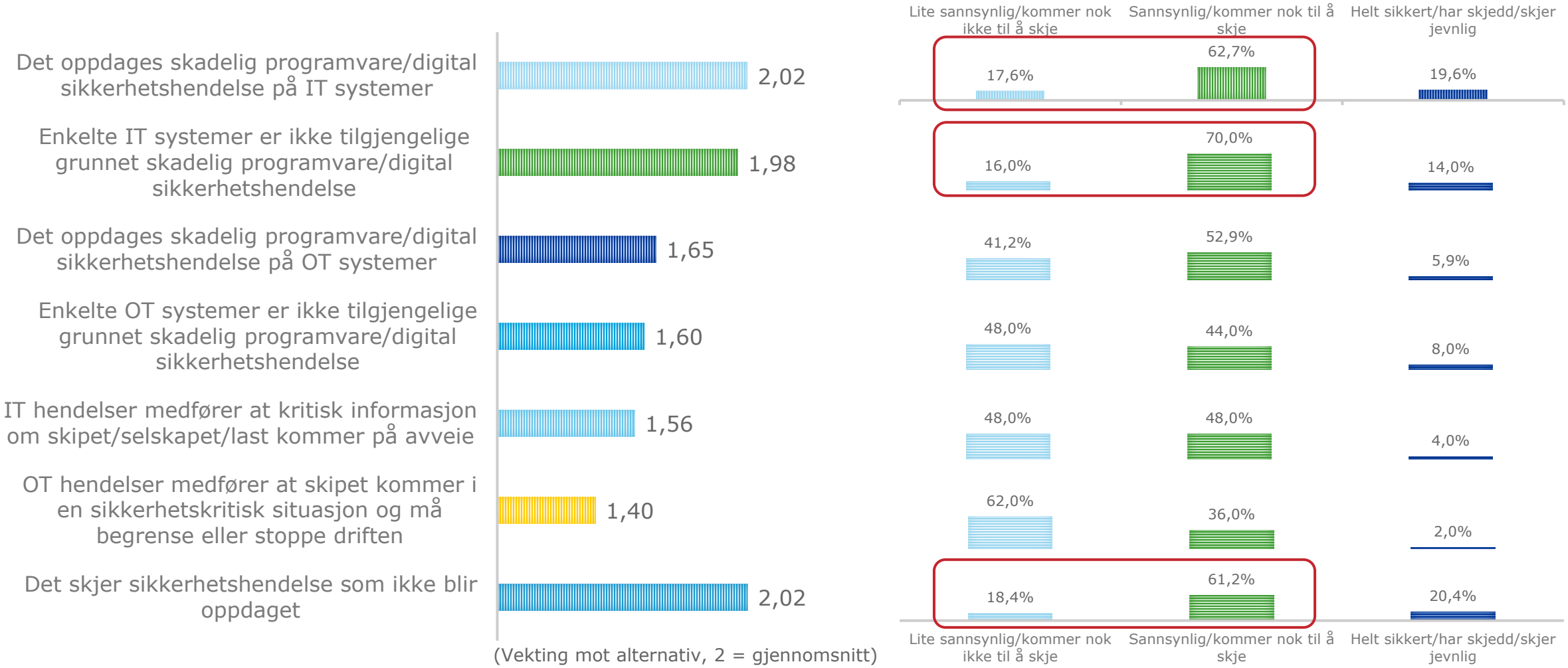
RR – Aggregert rest risiko

Fremdrift & styring	Konsekvens		Sannsynlighet / tilgang		IR	Tiltak	RR
Azipod'er	Systemfeil kan forårsake grunnstøting eller kollisjon	Kritisk	Høy tilgang - Fjerntilgang - USB porter - Nettverksforbindelse til andre systemer - Systemoppdateringer	Høy	Høy	Nettverkssegregering	Med
						Leverandørstyring og vedlikeholdsavtale med fokus på IKT sikkerhet Øvelser med fokus på IKT sikkerhetshendelser	Med /Lav
						Klare roller og ansvarligheter, og kompetente operatører	Lav



Bilde kilde: ABB Azipod propulsion

Hvilke konsekvenser av digitale sikkerhetshendelser om bord vil du vurdere som mest sannsynlige?



"IKT hendelser i IT systemer, og uoppdagede IKT hendelser anses som mest sannsynlig"

Sannsynligheten for en IKT-sikkerhetshendelse har sammenheng med trussel-agentens motivasjon, evner og mulighet (angrepsflate)

Trussel-agenter

+

Motivasjon

+

Evner

Infrastruktur

+ **Mulighet**
(sammenfallende Evner og kunnskap /tilgang til fysisk infrastruktur)

Typiske trussel-agenter for maritime skipssystemer

Kriminelle

Uforsiktige ansatte og leverandører

Misfornøyde ansatte

Konkurrenter

Aktivister

Statsaktører

Noen typiske trusler for maritime skipssystemer (1/2)

Skadevare

- Skadelig programvare eller skadelig programvare inkluderer virus, ormer, spionprogramvare, keylogger, osv.
- Angripere prøver vanligvis å stjele viktig informasjon eller å installere skadelig programvare for å få mer og mer kontroll over systemet ditt.
- Skadelig programvare kan infisere andre filer eller systemer. For eksempel er keyloggere en type malware designet for å fange opp alt du skriver - inkludert passordene dine - og sende de til angriperen.

Lagringsmedier

- USB-pinne eller nøkkelbrikker kan bli smittet ved å bare sette pinnen inn i en infisert datamaskin.
- En infisert USB-minnepinne infiserer alle andre maskiner den blir koblet til. Skadelig programvare sprer seg deretter til andre maskiner og nettverk. Vær alltid forsiktig når du oppbevarer USB-pinnene og andre datalagringsenheter. Stol aldri på USB-pinner du finner et sted. De kan bli infisert eller kan være nøye bygget angrepsenheter. Angripere lar dem ligge og håper at du vil hente dem og stikke dem inn i datamaskinen.
- Systemer som er kritiske for operasjoner, bør ikke ha åpne USB-porter. Hvis porten må være åpen, må IT-tjenestene dine deaktivere Autorun- eller Autoplay-funksjonene.

Løspengevirus

- Løsepengevirus krypterer filene på offerets datamaskin og krever løsepenger for å frigjøre dem. Dette er en stor trussel mot virksomheter som har mange virksomhetskritiske filer lagret i sine datasystemer, og dermed mister tilgang til dem.

Sosial manipulering

- Dyrbar informasjon kan brukes av angripere som deretter vil utgi seg for noen i nær kontakt med følget ditt eller være en kollega fra samme arbeidsgiver som deg, eller ved å annonsere falske jobbtilbud for å lure deg til et intervju for å få mer tilgang til sensitiv informasjon.
- Sosiale nettverksplattformer inneholder derfor en gullgruve med nyttig informasjon for angripere som ønsker lett bytte.

Kilde: NorSIS Trusler og trender 2019-2020, Wikipedia

Noen typiske trusler for maritime skipssystemer (2/2)

GPS spoofing

- **Et forsøk på å lure en GPS-mottaker ved å kringkaste falske GPS-signaler, strukturert til å ligne et sett med normale GPS-signaler, eller ved å kringkaste ekte signaler fanget andre steder eller på et annet tidspunkt. Disse falske signalene kan modifiseres på en slik måte at å få mottakeren til å estimere sin posisjon til å være et annet sted enn der den faktisk er, eller å være lokalisert der den er, men på et annet tidspunkt, som angitt av angriperen. En vanlig form for et GPS-spoofing-angrep, ofte kalt en bærer -off angrep, begynner med å kringkaste signaler synkronisert med ekte signaler observert av målmottakeren. Kraften til falske signaler økes deretter gradvis og trekkes bort fra ekte signaler. Et "proof-of-concept" -angrep ble vellykket utført i juni 2013, da luksusyachten White Rose of Drachs ble feildirigert med falske GPS signaler fra en gruppe luftfartsingeniørstudenter fra Cockrell School of Engineering ved University of Texas i Austin. Studentene var ombord på båten, slik at spoofing-utstyret deres gradvis kunne overmanne signalstyrken til de faktiske GPS-konstellasjonssatellittene og endre løpet av båten.**

Phishing

- Kriminelle lurer deg til å oppgi sensitiv informasjon om deg selv eller din virksomhet. Dataene brukes til ID-tyveri, utpressing og svindel, eller videreselges til andre kriminelle.
- En vanlig framgangsmåte er at en person sender en e-post og utgir seg for å være fra for eksempel en stor bank. E-posten sendes ut til en rekke personer og opplyser for eksempel om at det er problemer med noen kredittkort fra den banken. Problemet kan imidlertid, ifølge e-posten, løses lett ved å følge en vedlagt lenke til en nettside, svare på spørsmål der og fylle inn personalia og kredittkortinformasjon. Denne informasjonen brukes så til å tappe kredittkortet for penger. Det hele gjøres mer troverdig ved at e-posten ser ut som den er fra en anerkjent bank og at nettsiden man kommer til ser helt ut som de offisielle nettsidene til denne banken.
- Spear phishing er en selektiv, avansert og sofistikerte form for phishing. Den retter seg ofte mot bedrifter. Angriperen samler inn informasjon på forhånd, for eksempel om kunde, leverandør, avtaler og samarbeidspartnere. Denne informasjonen brukes så til å bygge kredibilitet i en e-post, ved å referere til interne ting og navn som er kjent for mottageren.

Man-in-the-middle

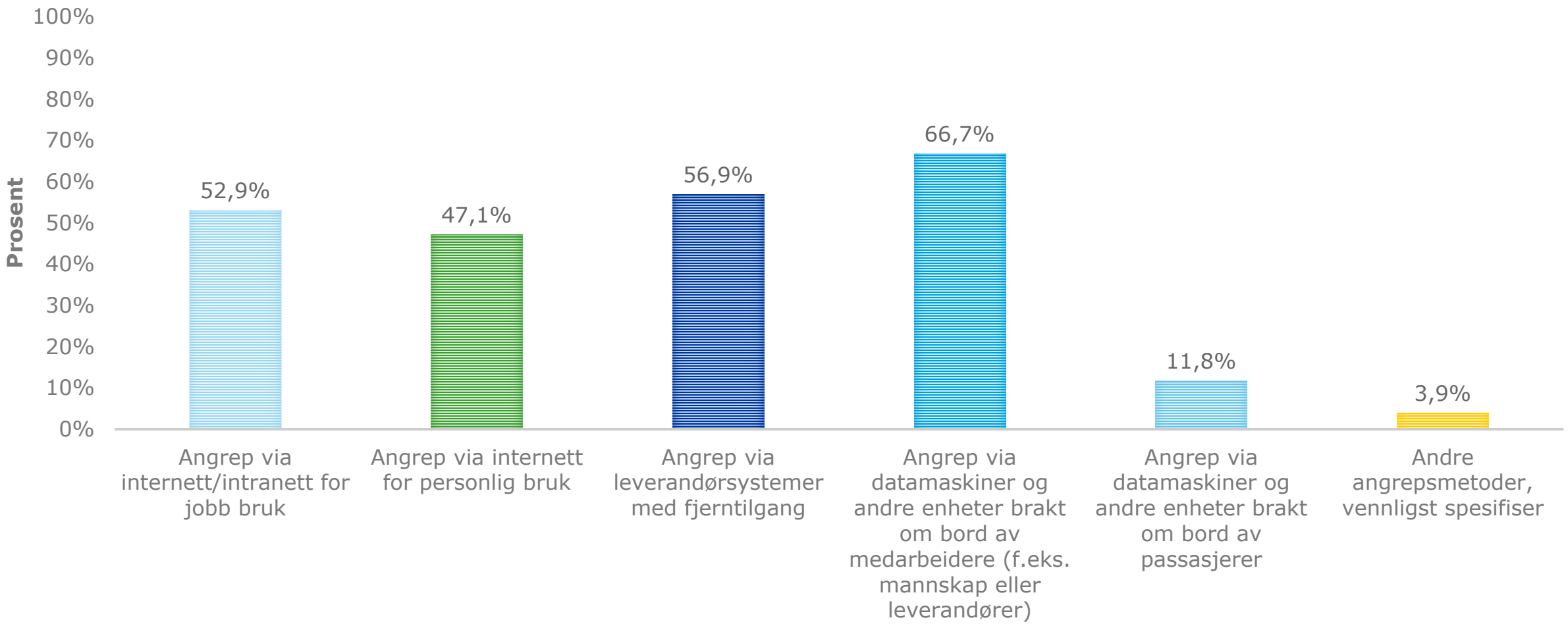
- Et man in the middle-angrep (MITM) er innen kryptografi og IT-sikkerhet et angrep hvor angriperen skjult releer og potensielt endrer kommunikasjonen mellom to parter som tror de kommuniserer direkte. Et eksempel på MITM-angrep er aktiv avlytting, hvor angriperen oppretter uavhengige forbindelser med ofrene og releer meldinger mellom dem for å få dem til å tro at de snaker direkte med hverandre over en privat forbindelse, mens faktum er at hele samtalen er kontrollert av angriperen. Angriperen må være i stand til å fange opp alle relevante meldinger mellom de to ofrene og injisere nye. Dette er rett frem under mange omstendigheter; for eksempel; en angriper innenfor mottaksradius av et ukryptert trådløst aksesspunkt (Wi-Fi) kan injisere seg selv som man-in-the-middle.

Session hi-jacking / Øktkapring

- Innefor IKT er øktkapring, (session hijacking) noen ganger også kjent som kapring av informasjonskapsler, utnyttelse av en gyldig dataøkt - noen ganger også kalt en økt-nøkkel - for å få uautorisert tilgang til informasjon eller tjenester i et datasystem. Spesielt brukes den til å referere til tyveri av en magisk informasjonskapsel som brukes til å autentisere en bruker til en ekstern server. Den har særlig relevans for webutviklere, da HTTP-informasjonskapsler som brukes til å opprettholde en økt på mange nettsteder lett kan bli stjålet av en angriper ved hjelp av en mellomliggende datamaskin eller med tilgang til de lagrede informasjonskapslene på offerets datamaskin. Etter å ha stjålet passende økt-cookies, kan en motstander bruke Pass the Cookie-teknikken til å utføre øktkapring.

Kilde: NorSIS Trusler og trender 2019-2020, Wikipedia

Hvilke angreps-metoder anser du for å utgjøre de største risikoene for digitale systemer ombord?



"Flere angreps-metoder er angitt med høy risiko, og gir et inntrykk av bredden og omfanget av utfordringen med å håndter IKT sikkerhetshendelser"

Maritim Digital Sikkerhet

Barrierer og modenhet i industrien

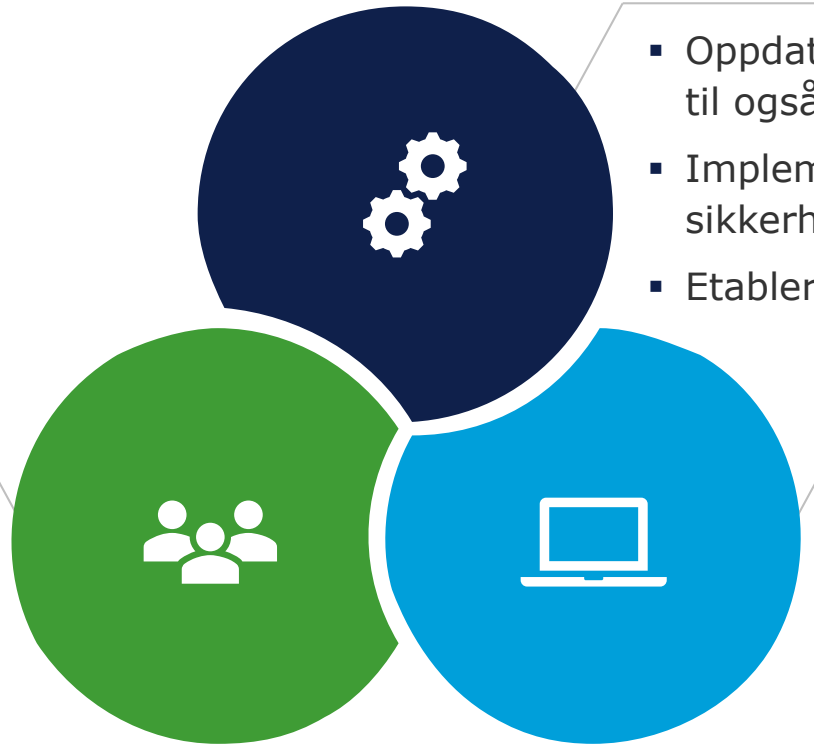
Anbefalt tilnærming for IKT sikkerhet på selskapsnivå bør være helhetlig og dekke menneske, organisasjon og teknologi

Vurder IKT sikkerhetsrisiko

Kontinuerlig verifikasjon av interne og/eller eksterne ressurser

Organisasjon

- Oppdatere styringssystemer for maritim sikkerhet til også å ta hensyn til IKT sikkerhet
- Implementere styringssystemet og etablere en IKT sikkerhetskultur
- Etablere hendelseshåndtering for IKT sikkerhet



Menneske

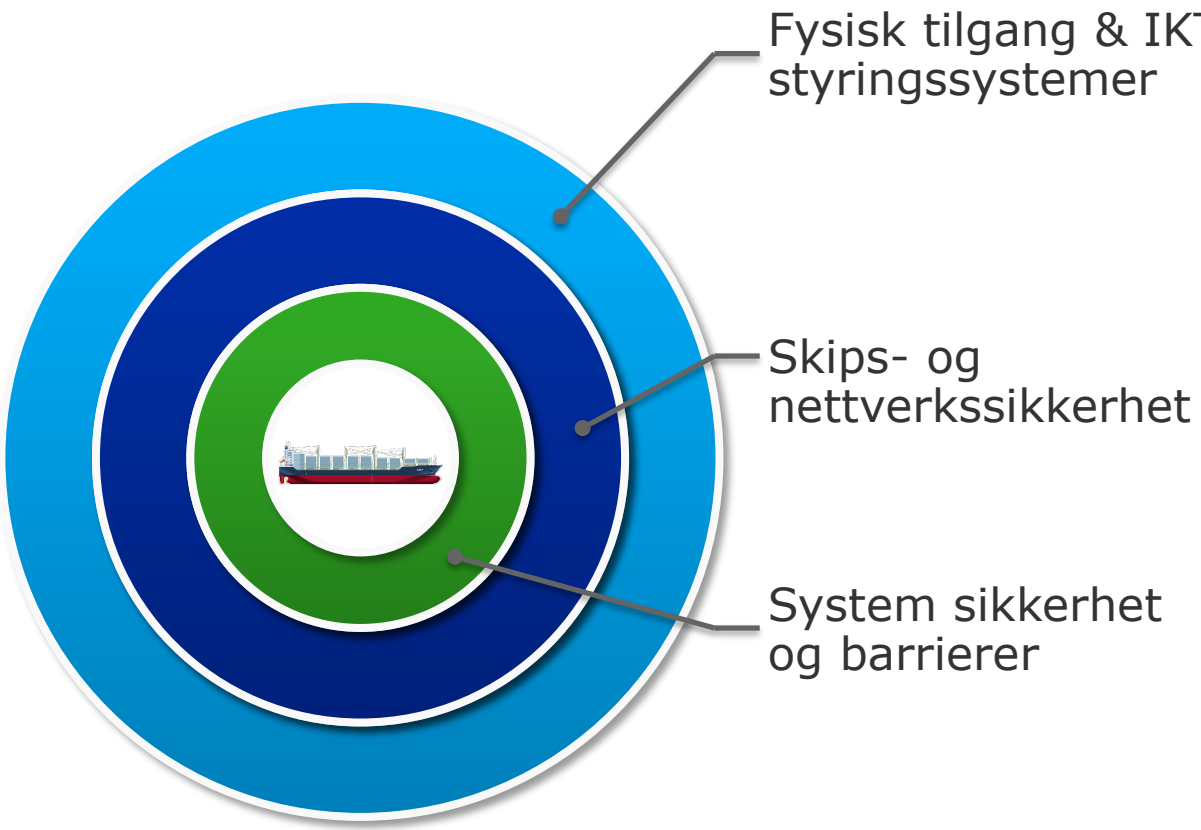
- Opplæring av ansatte om bord og på kontoret
- IKT sikkerhetsøvelser
- Definere roller og ansvarsområder

Teknologi

- Segregere kritiske systemer og usikre områder, og sørge for skallsikring
- Ta i bruk passende IKT sikkerhetstiltak på enkelt systemer

Det anbefales å bygge en IKT sikkerhetsmodell med flere lag av beskyttelse - IEC62443 sitt konsept med «Defence in Depth» er et godt utgangspunkt

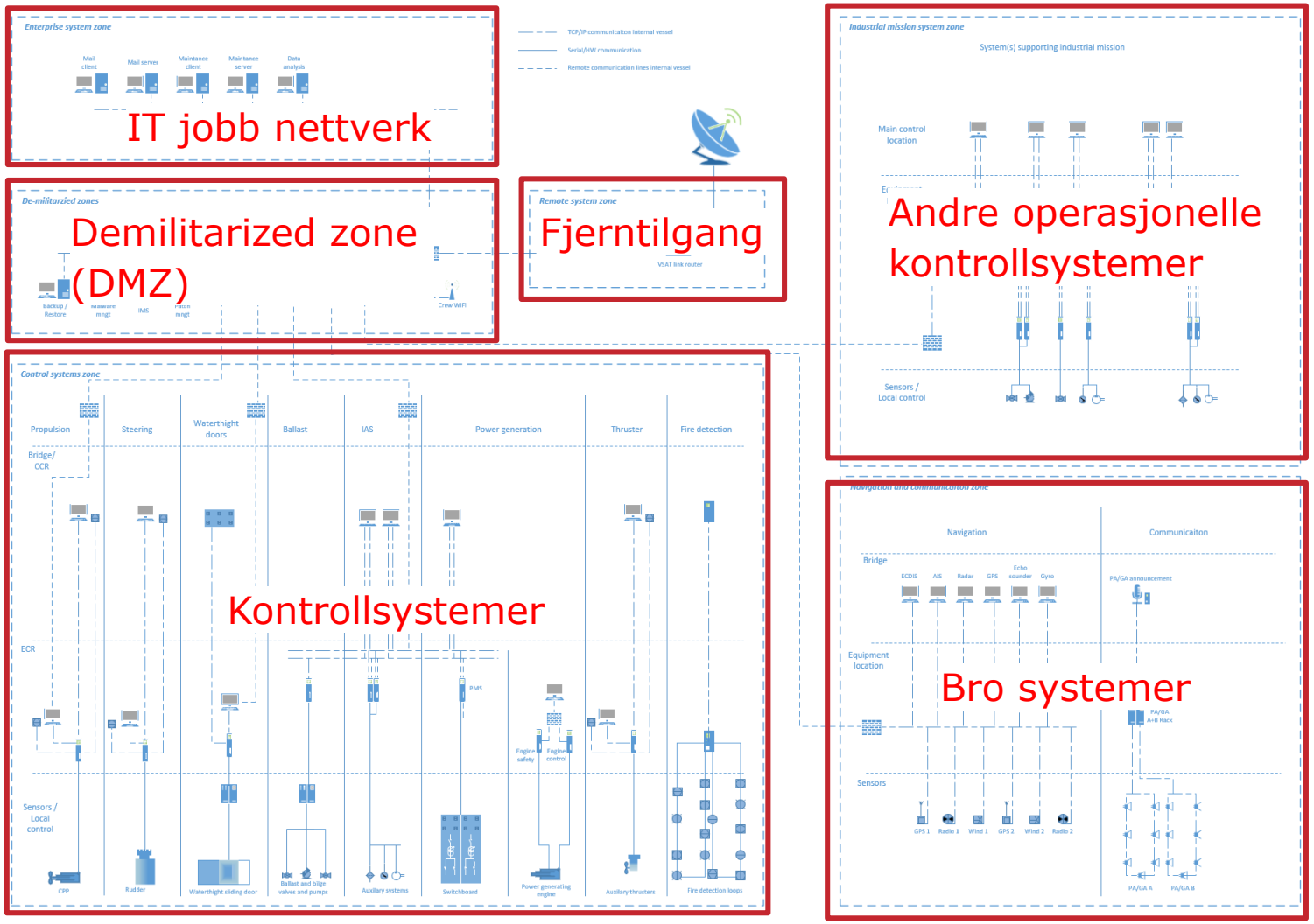
Defence in depth modellen



Flere lag støtter opp under en resistent modell

- **Fysiske og prosessuelle barrierer** *beskytter fartøysystemer ved hjelp av fysisk tilgang og prosedyrer (oppdateringer, adgangskort, låste skap, vedlikehold, "menneskelig brannmur", ...)*
- **Skipsbarrierer** *beskytter forbindelsen mellom soner og systemer med ekstern tilgangsstyring (VPN, DMZ, ...), segregering (brannmurer, datadioder, ...)*
- **Systembarrierer** *beskytter de enkelte systemene med barrierer som kryptering, brukerkontroll/autentisering, lagringsmedier, hendelseslogging, sikkerhetskopiering og gjenoppretting, etc.*

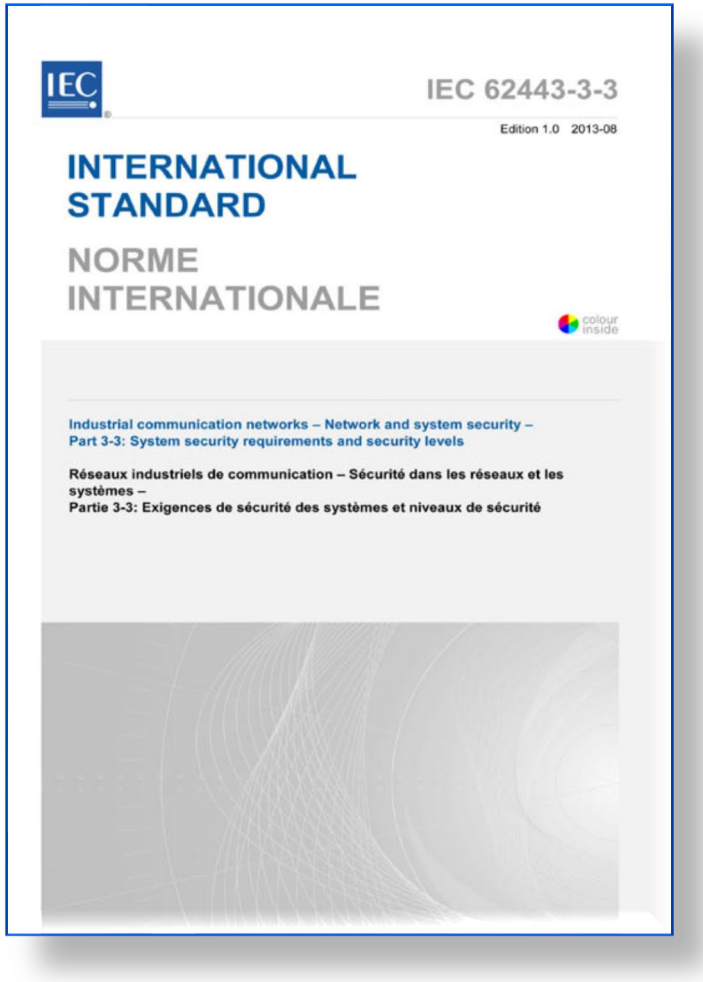
Nettverkssegregering og skallsikring er et av de viktigste tiltakene for å beskytte maritime kontrollsystemer



IEC62443-3-3 er en god og relevant standard for å vurdere IKT sikkerhets barrierer for kontroll systemer ombord

Tekniske krav i IEC62443-3-3 er ordnet etter 7 hovedkategorier:

- FR1 - Identification and authentication
- FR2 - Use control
- FR3 - Systems integrity
- FR4 - Data confidentiality
- FR5 - Restricted data flow
- FR6 - Timely response to events
- FR7 - Resource availability

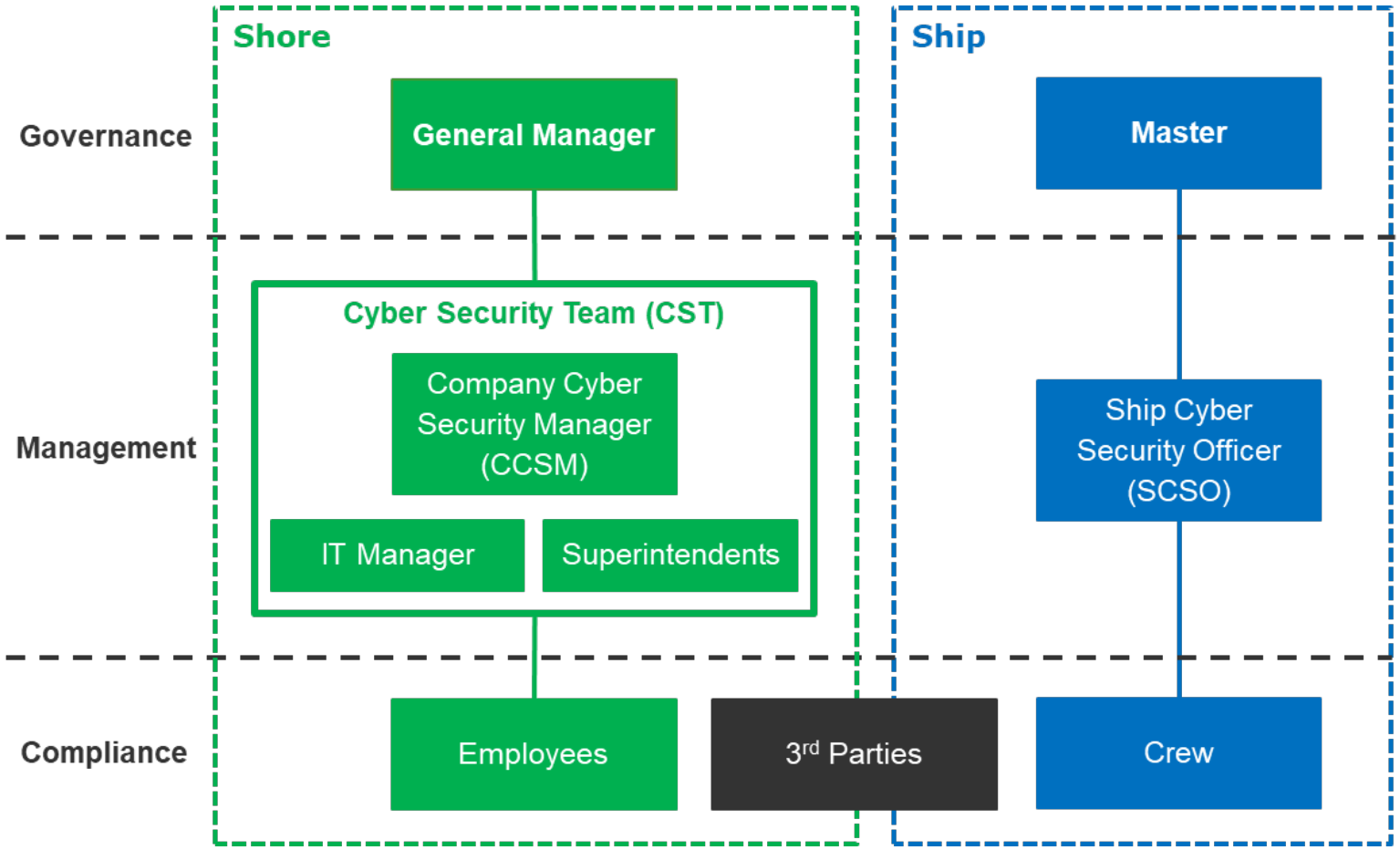


Et effektivt IKT styringssystem bør bygges rundt en anerkjent standard, ta hensyn til risiko og bygges rundt en kontinuerlig forbedringsprosess

1. **Identifisere**
   Definer personalets roller og ansvar for styring av IKT risiko og identifiser systemene, eiendelene, dataene og evnene som, når de forstyrres, utgjør en risiko for skipets drift
2. **Beskytte**
   Implementer risikoprosesser, tiltak og beredskapsplaner for å beskytte mot IKT hendelser og sikre kontinuitet i skipsdriften
3. **Oppdage**
   Utvikle og implementer aktiviteter som er nødvendige for å oppdage en IKT hendelse i tide
4. **Respondere**
   Utvikle og implementere tiltak og planer for å øke motstandsdyktighet og gjenopprette systemer for skipsdriften svekket på grunn av en IKT hendelse
5. **Gjenopprette**
   Identifiser tiltak for å sikkerhetskopiere og gjenopprette IKT systemer som er nødvendige for skipsdriften som er påvirket av en IKT hendelse

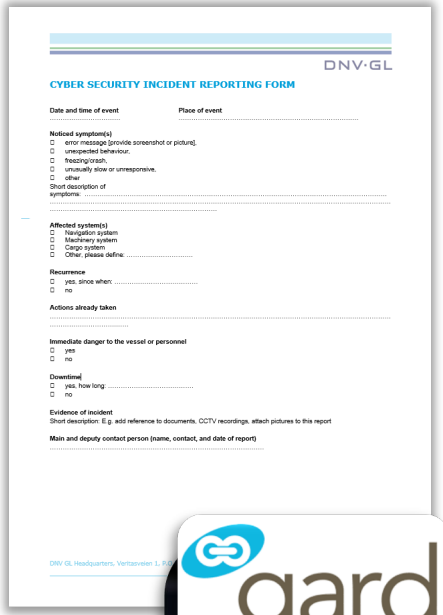
Definere roller og ansvar, og forankre IKT sikkerhet hos toppledelsen

- **Definer en organisasjon** for IKT sikkerhet (på land & ombord)
- **Bygge på nåværende struktur** av roller og ansvar
- **Identifiser ressurser** som kan fyller de nye rollene
- **Definer oppgaver**, ansvar og kommunikasjonslinjer
- **Forankre IKT sikkerhet** hos toppledelsen



Opplæring og bevissthet om IKT sikkerhet, og hendelseshåndtering

- «***Den menneskelige brannmuren***» kan være ditt sterkeste forsvar, eller ditt svake punkt ifm. IKT sikkerhet
- **Anbefalte former for opplæring**/bevissthet fokus:
  - **Bevissthet om IKT sikkerhet** for både skips- og kontorpersonell (videoer, nyheter, briefing, …)
  - Mer **utdypende opplæring for IKT sikkerhets ansvarlig** personell både om bord og på kontoret
  - **IKT sikkerhetsøvelser** øker beredskapen og avdekker manglende tiltak
- Implementere en **strukturert tilnærming til hendelseshåndtering**
  - **Øve** på hendelseshåndtering
  - **Promotere en «no-blame» kultur** med aktiv rapportering
  - Lage **brukervennlige prosesser** for rapportering


DNV·GL

CYBER SECURITY INCIDENT REPORTING FORM

Date and time of event

Place of event

Noticed symptom(s)
- ☐ error message [provide screenshot or picture],
- ☐ unexpected behaviour,
- ☐ freezing/crash,
- ☐ unusually slow or unresponsive,
- ☐ other

Short description of symptoms:

Affected system(s)
- ☐ Navigation system
- ☐ Machinery system
- ☐ Cargo system
- ☐ Other, please define:

Recurrence
- ☐ yes, since when:
- ☐ no

Actions already taken

Immediate danger to the vessel or personnel
- ☐ yes
- ☐ no

Downtime
- ☐ yes, how long:
- ☐ no

Evidence of incident
Short description: E.g. add reference to documents, CCTV recordings, attach pictures to this report

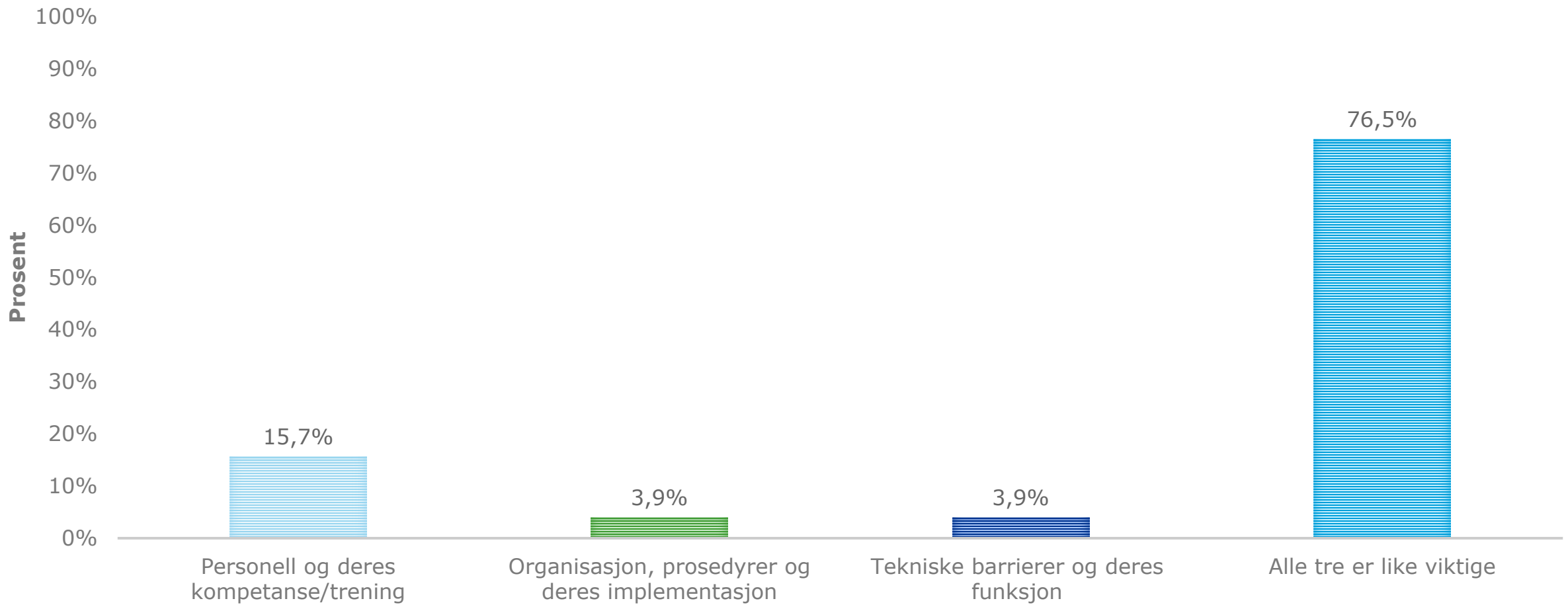
Main and deputy contact person (name, contact, and date of report)

DNV GL Headquarters, Veritasveien 1, 1322

www.dnvgl.com/csvideo

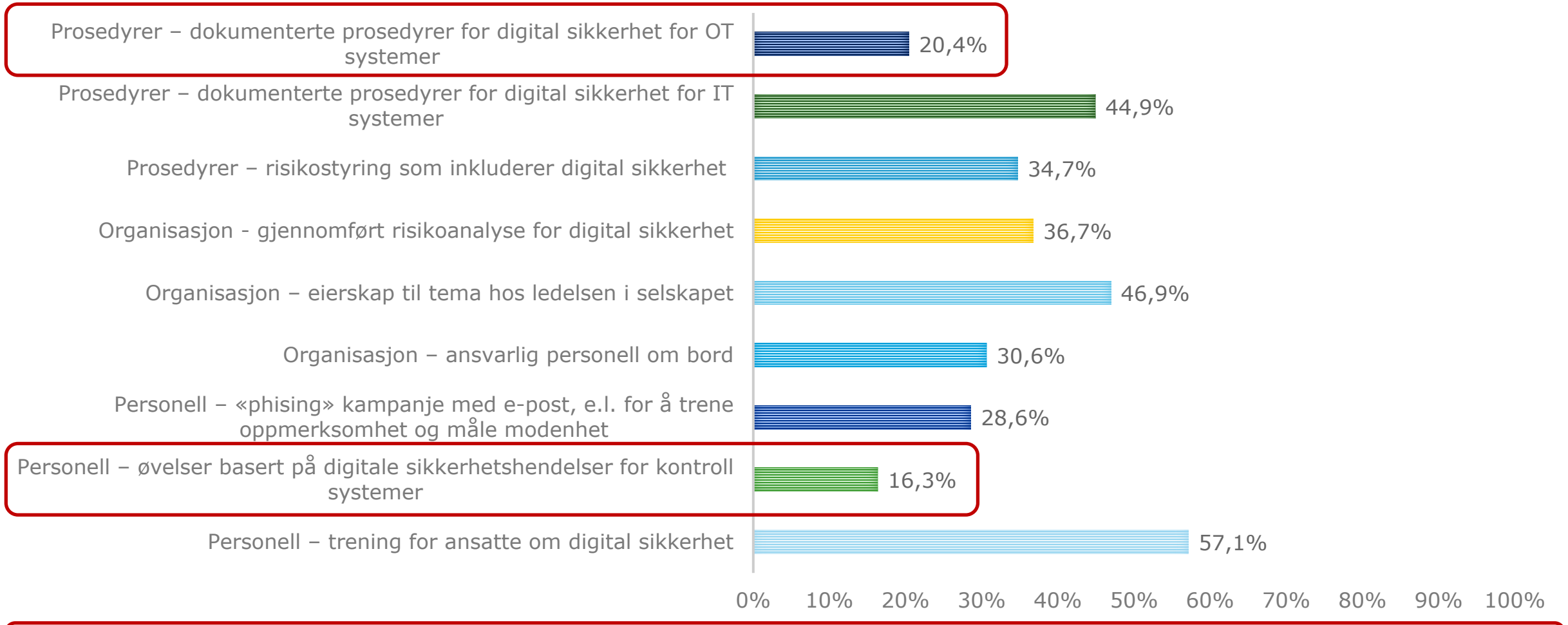
For å redusere digitale sikkerhetstrusler, bygges gjerne tiltak rundt de tre områdene personell, prosedyrer og teknologi

Hvilket område vurderer du som det viktigste?



"Det er god forståelse for at IKT risiko må håndteres på en helhetlig måte med å bygge kompetanse, etablere styringssystemer og implementere tekniske tiltak

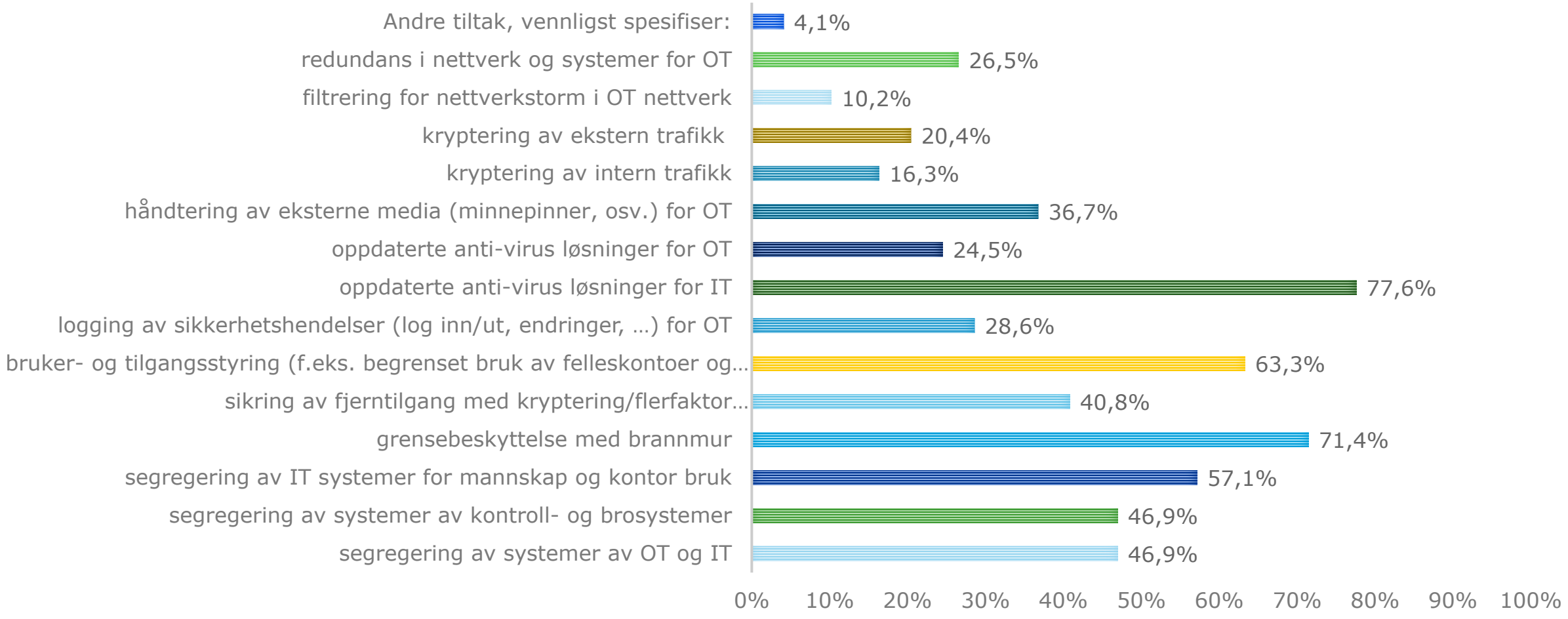
Hvilke tiltak er allerede utført for deres flåte?
- Organisasjon, prosedyrer og personell



"God forankring i ledelsen, og høy modenhet med tanke på tiltak, spesielt for IT systemer. Når det kommer til OT systemer, gjenstår det fortsatt en del arbeid med etablering av styringssystemer og beredskap."

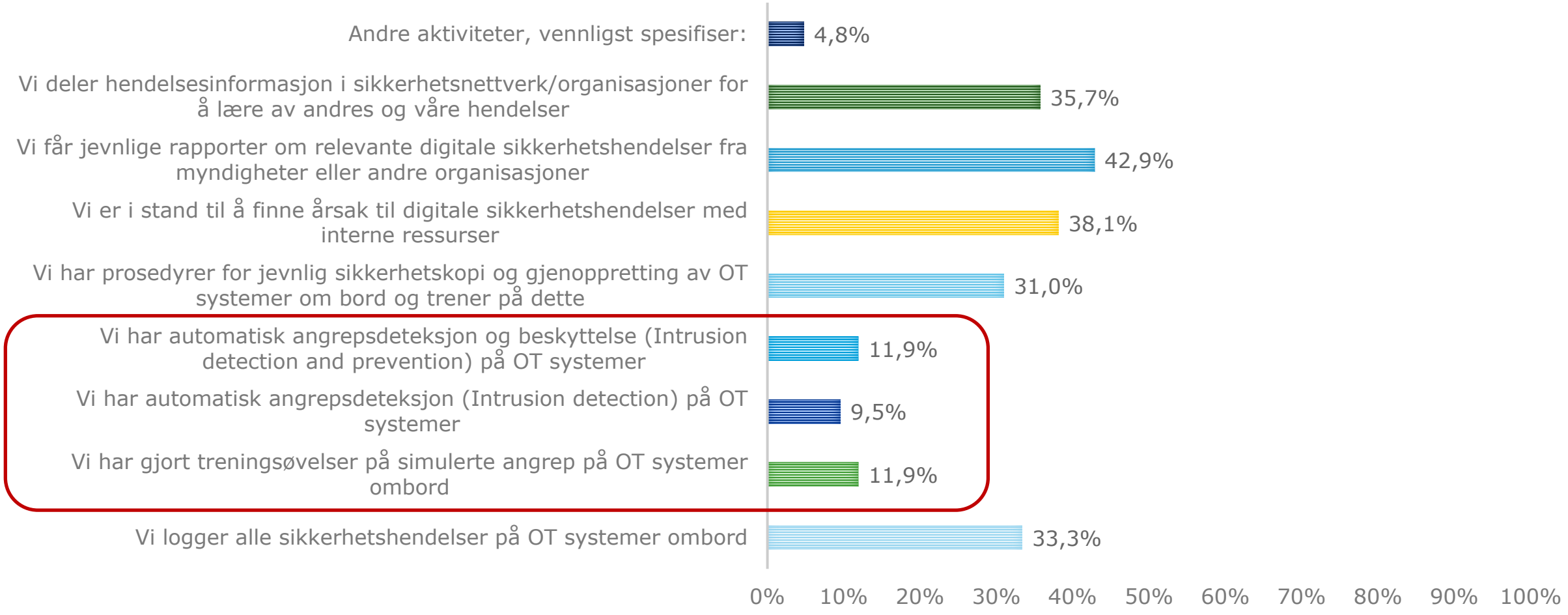
Hvilke tiltak er allerede utført for deres flåte?
- Teknologi

Teknologi



"Også for tekniske tiltak er det tydelig at IT systemer er mer modne enn OT systemer."

Hvor godt forberedt mener du at dere er til å håndtere digitale sikkerhetshendelser for OT systemer om bord?



"Deling av erfaringer og bruk av tilgengelig rapporter er utbredt for IKT sikkerhetshendelser. Også for hendelseshåndtering er det et forbedringspotensial for OT systemer."

Modenhetsvurdering kan baseres på anerkjente standarder, og vi vurderer OT sikkerhets-modenhet til å ligge betydelige etter IT sikkerhet-modenhet

Level	CMMI-SVC	ISA-62443-2-2	Description	Modenhetsvurdering
1	Initial	Initial	At this level, the models are fundamentally the same. Processes are performed in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency over time may not be able to be shown. Note: "Documented" in this context refers to the procedure followed in performing this activity (for example detailed instructions to personnel), not to the results of performing the process.	IKT sikkerhet for (OT) kontroll- og bro systemer
2	Managed	Managed	At this level, the models are fundamentally the same, with the exception that ISA-62443-2-2 recognizes that there may be a significant delay between defining a process and executing (practicing) it. Therefore, the execution related aspects of the CMMI-SVC Level 2 are deferred to Level 3. At this level, the organization has the capability to manage the delivery and performance of the service according to written policies (including objectives). The discipline reflected by Maturity Level 2 helps to ensure that security practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.	
3	Defined	Defined (Practiced)	At this level, the models are fundamentally the same, with the exception that the execution related aspects of the CMMI-SVC Level 2 are included here. Therefore, a process at Level 3 is a Level 2 process that is being practiced on the IACS. The performance of a Level 3 security practice can be shown to be repeatable over time within the IACS.	IKT sikkerhet for IT-systemer
4	Quantitatively Managed Optimizing	Improving	At this level, the "Quantitatively Managed" and "Optimizing" CMMISVC levels are combined. Using suitable process key performance indicators, the effectiveness and/or performance improvements of the process can be demonstrated. This results in a security program that improves the process through technological, procedural or management changes.	

IKT sikkerhet for OT systemer utføres ofte ad-hoc, og det er begrenset med dokumenterte prosesser. For IT systemer, er prosedyrene for det meste på plass og blir fulgt.

Maritim Digital Sikkerhet

Mulige tiltak og veien videre

Hvilken støtte ønsker dere fra myndighetene og andre aktører i maritim bransje for å håndtere digital sikkerhet?

Regelverk og tilsyn

- Fortrinnsvis bør regler om Cyber Security være praktisk orientert, også for de enklere digitale fartøyene.
- Cyber Security fremstår som et regelverk designet for større aktører med store konsekvenser.
- Andre bør støttes i nedskalerte prosedyrekrav, kompetansekrav og treningskrav.
- Ingen, kun mindre spørsmål og mindre prosedyrer påtvunget av myndighetene. Byråkratiet i sjøfartsdir er allerede for omfattende.
- Vi ønsker at myndighetene og organisasjonene tar grep for å sikre datasikkerheten på fiskebåter, slik at ikke IT konflikter går ut over sikker drift av flåten.

Teknisk

- Brannmurer og eller andre barrierer i nettverk som er retta mot industrien.
- Tydeligere krav til sikkerhet i OT systemer.

Leverandører

- Få leverandører av OT systemer til automatisk å sende oss informasjon om sikkerhetskritiske oppdateringer, samt at de oppdaterer OS når de også oppdaterer software ifm. service - Her må de virkelig flagge med viktigheten av oppdateringen og finne balansegangen, så en ikke må oppdatere for ofte da en oppdatering er en risiko i seg selv pga. mulig teknisk feil.
- Pga. av dette, må vi bli mindre avhengig av servicefolk for å kunne oppdatere software, men at software automatisk sikkert kan lastes ned i en "boks" og crew velger når de skal starte den automatiske oppdateringen.

Veiledning

- Ønsker gjerne mer informasjon og rettleiing angående.
- Ønsker hjelp til systematisk tilnærming til temaet for skip/rederi i handelsflåten.
- Bransjestandard med konkrete råd og tiltak. Best practices.

Innspill til mulige tiltak for å øke maritim digital sikkerhet

Regelverk

- Regelverk for maritim digital sikkerhet bør **være i tråd med internasjonale lover og regler** grunnet industriens internasjonale karakter for å unngå konkurranse vridning

Veiledning

- **Veiledning innen de viktige områdene for IKT sikkerhet bør støttes av sjøfartsdirektoratet**. F.eks. innen styringssystemer, tekniske barrierer, og kompetanse
- For **mindre aktører** kan sjøfartsdirektoratet gjøre et viktig bidrag med å **støtte opplæring og samarbeid**

Teknisk

- Industrien trenger også **støtte til å utvikle og introdusere passende tekniske IKT sikkerhetstiltak**
- **Leverandør industrien** i Norge vil også ha behov for **støtte til å implementer IKT sikkerhet** i sine systemer

ROS analyse for maritim digital sikkerhet

Sårbarhetsanalyse forbindelse med strategi for maritim digital sikkerhet

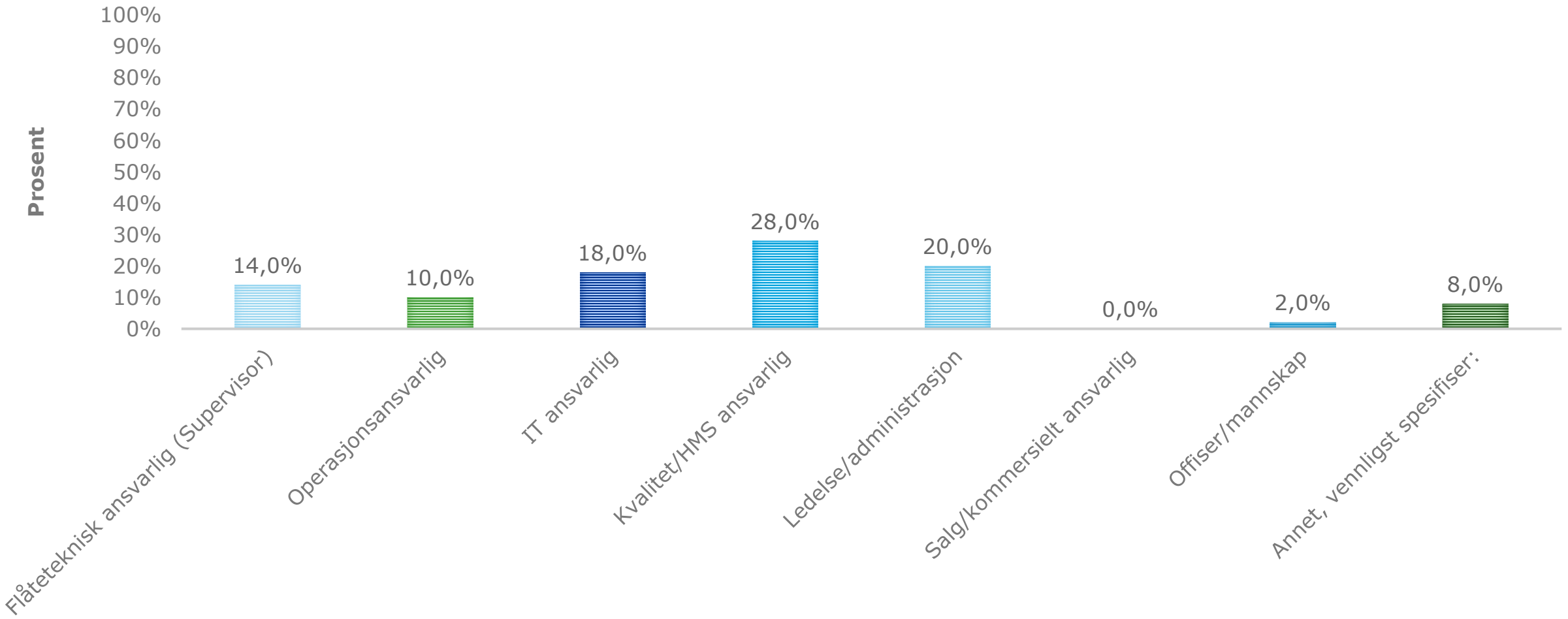
Jarle Blomhoff, Group Leader Cyber Safety & Security
jarle.blomhoff@dnvgl.com
+47 970 61 347

www.dnvgl.com

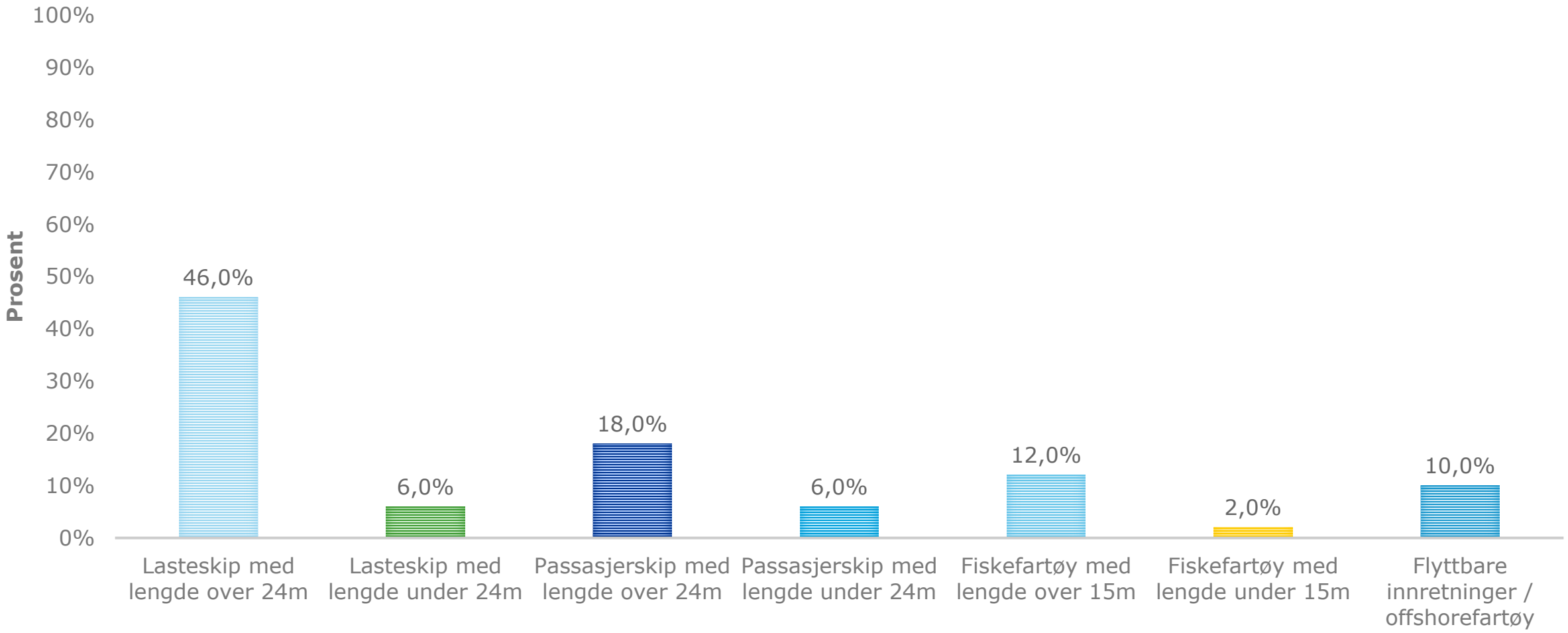
SAFER, SMARTER, GREENER

VEDLEGG - Spørreundersøkelse

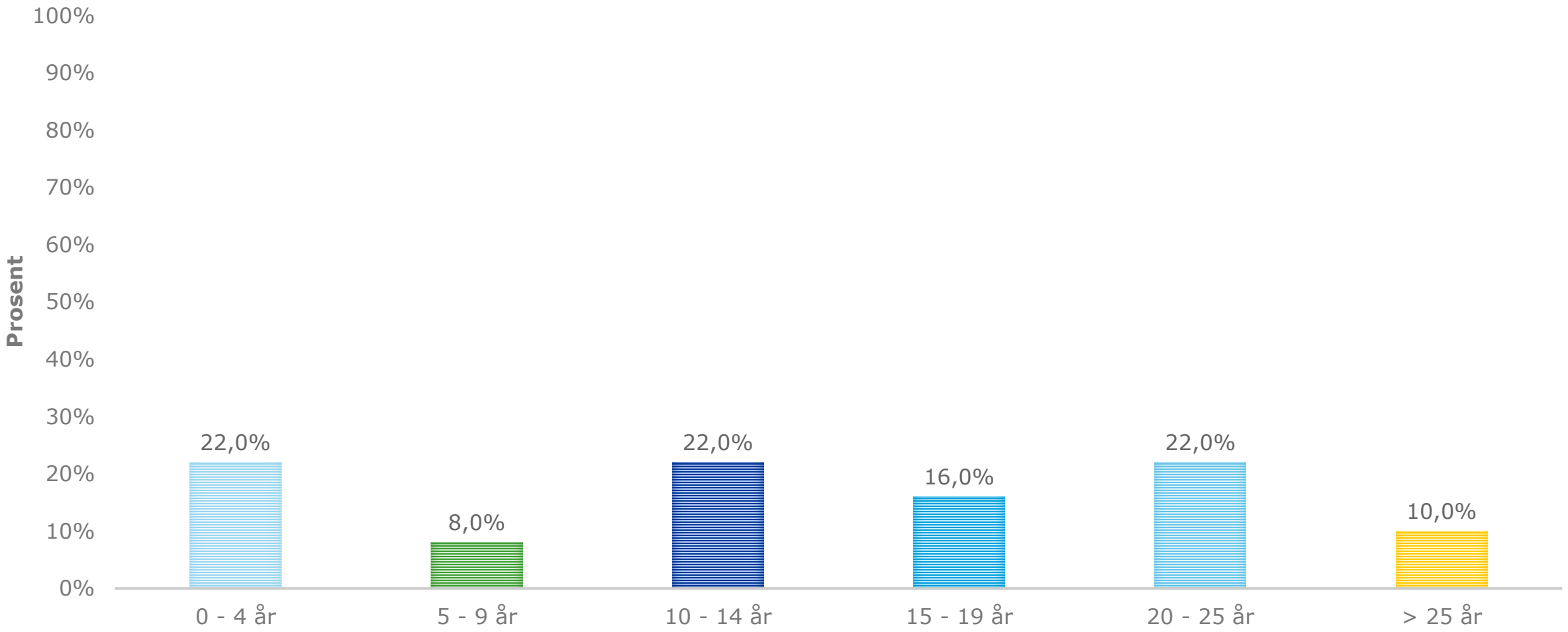
Hva er din rolle i organisasjonen?



Hvilken av hovedkategoriene av skipstyper tilhører hoveddelen av flåten deres?



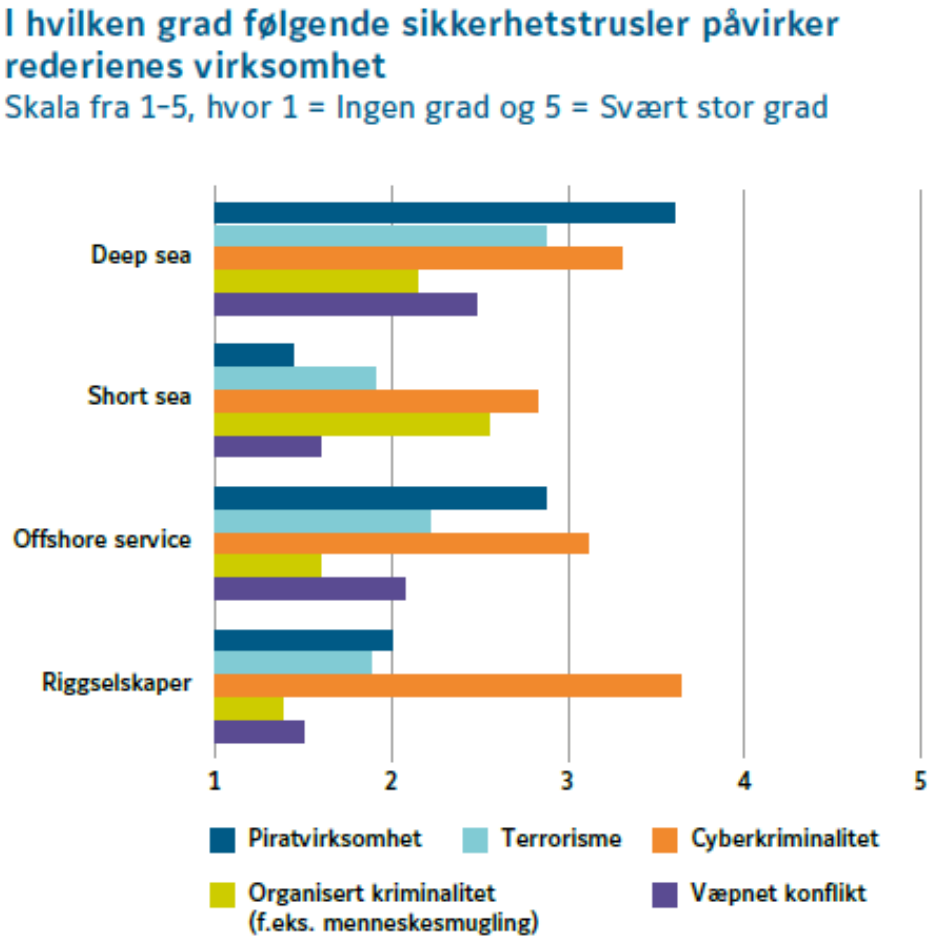
Hvor mange år har du jobbet innen dette fagområdet?



VEDLEGG – Andre kilder

Kilde – «Norges Rederiforbund – Konjunkturrapport 2019»

- «**Cyberkriminalitet** den alvorligste sikkerhetstrusselen *I medlemsundersøkelsen ble rederiene spurt om i hvilken grad deres operasjoner blir påvirket av sikkerhetstruslene fra piratvirksomhet, terrorisme, cyberkriminalitet, organisert kriminalitet, væpnet konflikt og geopolitiske spenninger. Fire av ti oppgir at cyberkriminalitet påvirker deres operasjoner i stor eller svært stor grad.»*
- *«64 prosent av riggselskapene sier at trusselen om cyberkriminalitet vil påvirke deres operasjoner i stor eller svært stor grad. Rett under halvparten av deep sea-rederiene sier det samme.»*
- «Det er grunn til å anta at utfordringer knyttet til cyberkriminalitet vil bli en stadig mer relevant problemstilling, etter hvert som flere virksomheter tar i bruk ytterligere digitaliserte, automatiserte og autonome tjenester. IKT sikkerhet er ikke sett på som den største barrieren for automatisering.»



Kilde – «Safety at Sea and BIMCO cyber security white paper 2019» (1/2)

What was the impact of any cyber breaches?

48%
Loss of corporate data

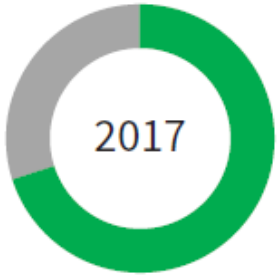
67%
IT system functionality

21%
Financial loss

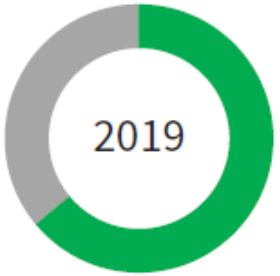
4%
Shipborne system functionality

Source: Survey 2016

Do you provide cyber-risk awareness training to staff?



Yes 70%
No 30%



Yes 64%
No 36%

Source: Survey 2017, 2019

What form does that training take?

53 Internal training course

20 Training by external provider

11 Cyber crisis management exercises

Source: Survey 2019 (Sample size 72, multiple responses accepted)

Kilde – «Safety at Sea and BIMCO cyber security white paper 2019» (2/2)

Were protection strategies in place before the attack?

Yes 74%

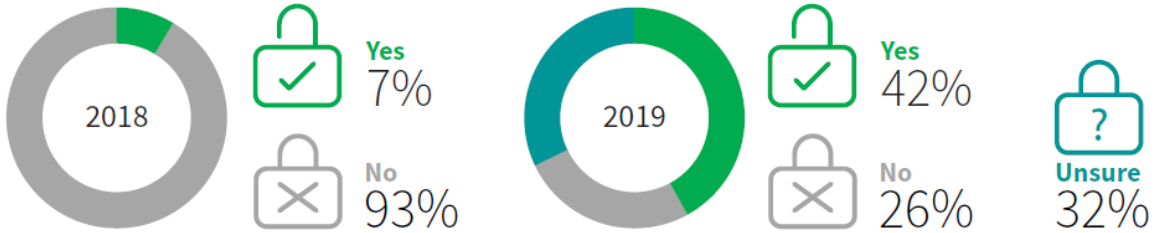
No 26%

What is in place to protect against cyber attack?

Firewalls	74%
Intrusion detection/prevention system	45%
Best practice protocols	39%
Physical segregation of networks	30%
Review of log files	21%
Virtual segregation of network nodes	18%
Independent cyber security consultants	15%
Other	11%

Source: Survey 2016

Does your company protect your vessels from OT cyber threats?



Source: Survey 2019

Overall, how do you rate cyber risk to your organisation?

High	Medium	Low
41%	41%	28%

Does your organisation have a business continuity plan in the event of a cyber incident?

(Sample size: 176)

Yes 52% No 19% Unsure 29%

When was the business continuity plan last tested? (months)

<3	3–6	6–12	>12	Not tested
23%	24%	17%	14%	32%

Source: Survey 2019

Does your organisation have a dedicated hotline for reporting cyber incidents?

Yes 68% No 18% Unsure 14%

Source: Survey 2019 (Sample size: 101)

Would you stop doing business with suppliers of systems if the cyber resilience of their products was called into question?

Yes 83% No 17%

Source: Survey 2019 (Sample size: 160)

Kilde – «SANS 2019 State of OT/ICS Cybersecurity review» (1/2)

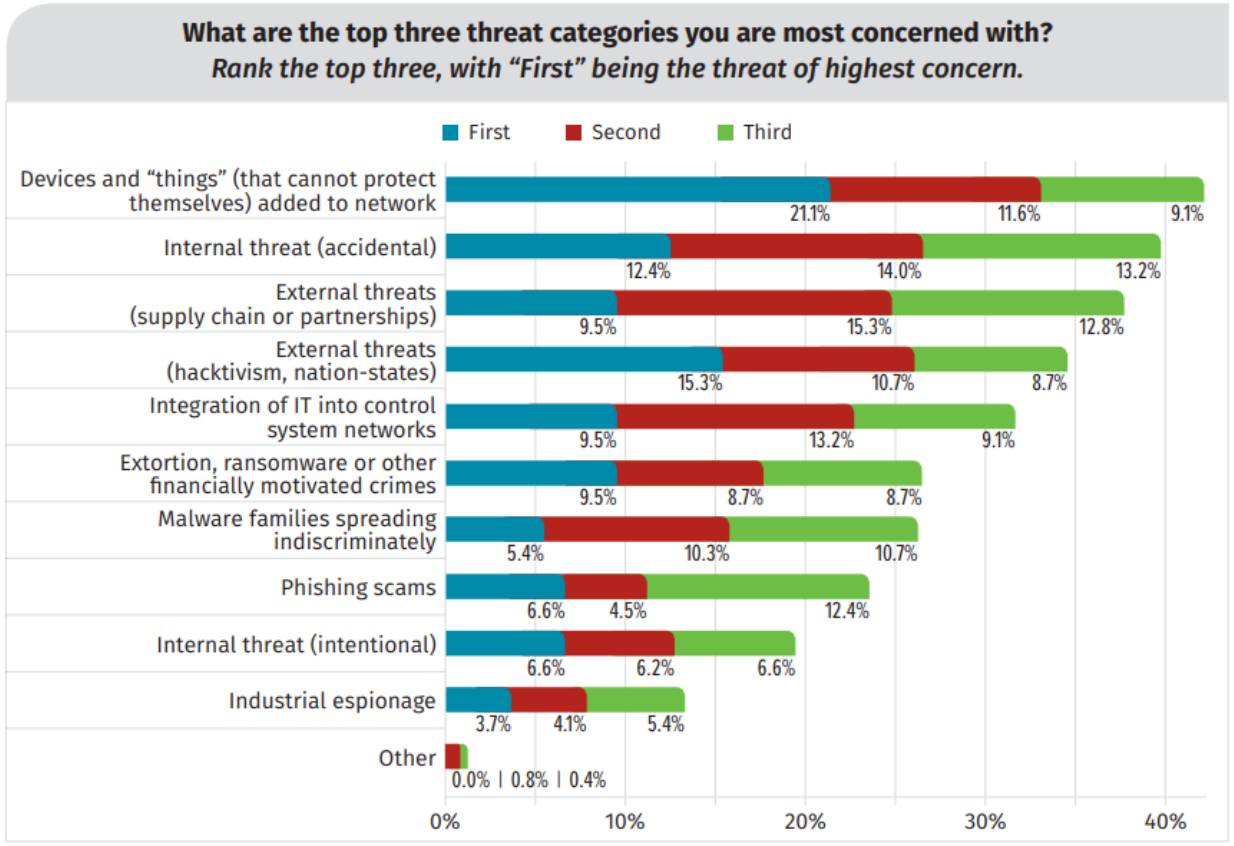


Figure 3. Leading Threat Categories

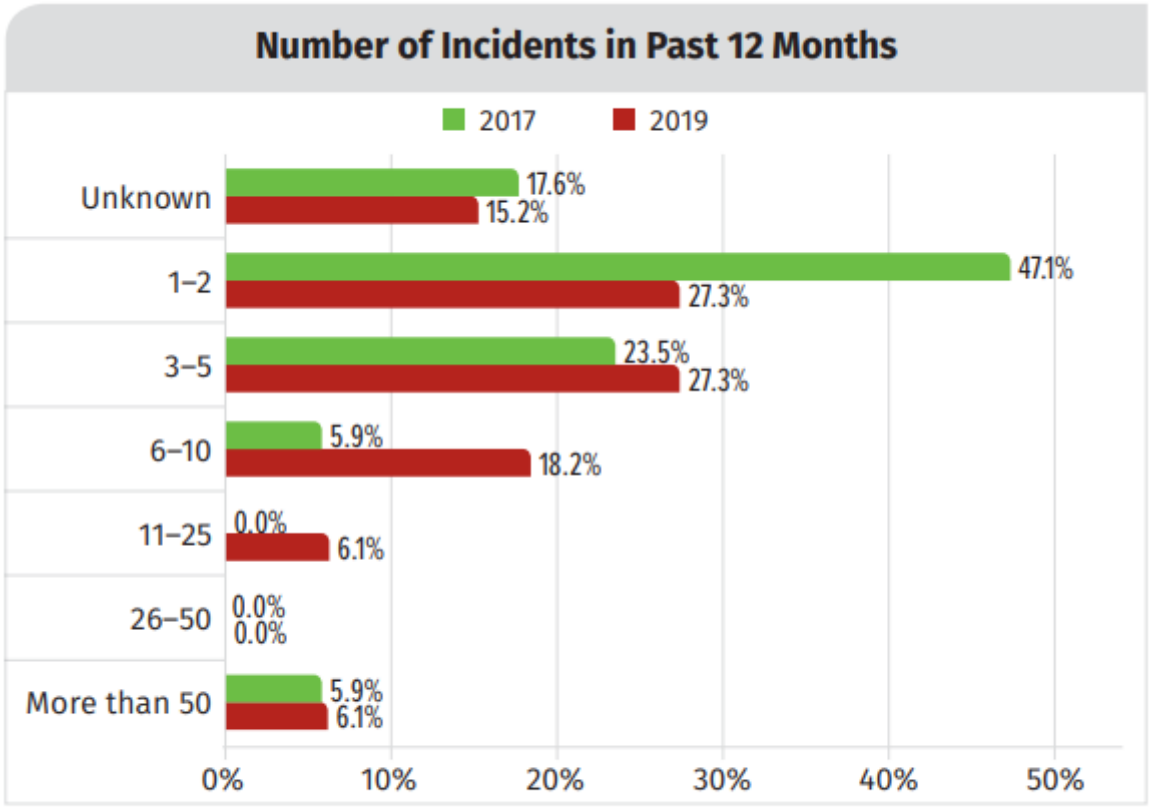


Figure 4. Comparison of OT/Control System Incidents 2017 vs. 2019

Kilde – «SANS 2019 State of OT/ICS Cybersecurity review» (2/2)

Table 2. Actors Involved in Incidents

	2017	2019
Intentional Malicious		
Hackers	56.3%	44.8%
Foreign nation-states or state-sponsored parties	0.0%	27.6%
Organized crime	0.0%	24.1%
Activists, activist organizations, hacktivists	12.5%	17.2%
Competitors	12.5%	10.3%
Former employees	0.0%	10.3%
Former equipment providers	0.0%	6.9%
Both/Unknown		
Current employees	31.3%	34.5%
Unknown (sources were unidentified)	31.3%	17.2%
Unintentional		
Current service providers, consultants, contractors	12.5%	31.0%
Nonmalicious actors (internal)		20.7%
Current equipment providers	18.8%	13.8%
Domestic intelligence services	0.0%	6.9%
Suppliers or partners	12.5%	6.9%

Table 3. Timeline for Compromise to Remediation 2019

Step	Timeline	Percentage
Compromise to Detection	2 to 7 days	44.8%
Detection to Containment	6 to 24 hours	53.6%
Containment to Remediation	2 to 7 days	53.9%

Table 4. Initial Attack Vectors 2019

	% Response
Physical access (USB stick, direct access to equipment)	56.3%
Remote access (bypassing intended architecture)	40.6%
Trusted remote access (through intended architecture)	37.5%
Service maintenance and consulting (configuration changes)	34.4%
Supply chain (i.e., altered/modified hardware or software; software/firmware updates and patches; maintenance tools/equipment)	18.8%

Kilde – «The Maritime Executive» and NavalDome

The Maritime Executive
INTELLECTUAL CAPITAL FOR LEADERS

Naval Dome: Cyberattacks on OT Systems on the Rise

BY THE MARITIME EXECUTIVE 07-26-2020 07:18:37

The maritime industry's operational technology (OT) systems are vulnerable to a rising number of cyberattacks, with incidents expected to reach record volumes by the year's end. Attacks on maritime stakeholders have already increased by 900 per cent over the last three years, according to Israeli cybersecurity firm Naval Dome.

In 2017 there were 50 significant OT hacks reported, increasing to 120 in 2018 and more than 310 last year. 2020 is expected to end with more than 500 major cybersecurity breaches, with substantially more going unreported.

At the AAPA's 2020 Port Security Seminar & Expo, Robert Rizika, Naval Dome's Boston-based head of North American operations, said that since NotPetya – the virus that resulted in a $300 million loss for Maersk – attacks are increasing at an alarming rate.

Recalling recent incidents, he told delegates that in 2018 the first ports were affected, with Barcelona, then San Diego falling under attack. Australian shipbuilder Austal was hit and the attack on COSCO took down half of the shipowner's US network.

This year, a U.S.-based gas pipeline operator and shipping company MSC have been hit by malware. The latter incident shut down the shipowner's Geneva HQ fo five days. A U.S.-based cargo facility's operating systems were infected with the Ryuk ransomware, and last month the OT systems at Iran's Shahid Rajee port were hacked, restricting all infrastructure movements and creating a massive bacl log.

The spate of attacks has raised public awareness of the potential wider impact of cyber threats on ports around the world. Intelligence from Iran, along with digital satellite imagery, showed the Iranian port in a state of flux for several days. Dozens of cargo ships and oil tankers waiting to offload, while long queues of trucks formed at the entrance to the port stretching for miles, according to Naval Dome.

Emphasising the economic impact and ripple effect of a cyber-attack on port infrastructure, Rizika said that a report published by Lloyd's of London indicated that if 15 Asian ports were hacked, financial losses would be more than $110 billion - a significant amount of which would not be recovered through insurance policies, as OT system hacks are not covered.

All parts of the OT system – the network connecting RTGs, STS cranes, traffic control and vessel berthing systems, cargo handling and safety and security systems – are under threat.

"Unlike the IT infrastructure, there is no "dashboard" for the OT network allowing operators to see the health of all connected systems. Operators rarely know if an attack has taken place, invariably writing up any anomaly as a system error, system failure, or requiring restart. They don't know how to describe something unfamiliar to them. Systems are being attacked but they are not logged as such and, subsequently, the IT network gets infected," Rizika said.