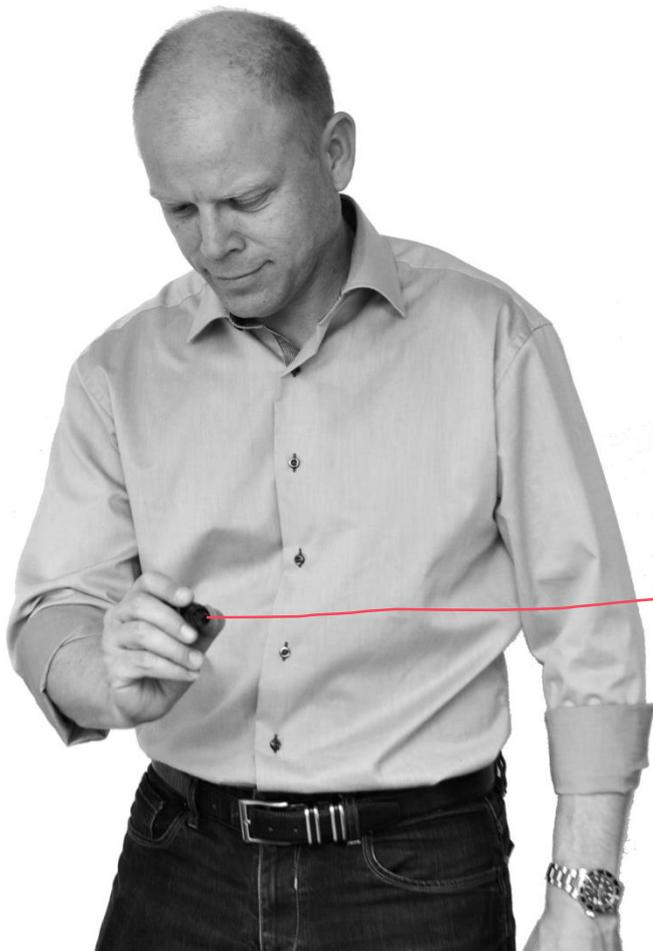


Hvad gør jeg, når min virksomhed bliver ramt?_

DI Digital medlemsmøde, Herning

Frederik Helweg-Larsen, Expert Director
15. oktober 2019



Frederik Helweg-Larsen

Expert Director, Risk & Security

fhl@devoteam.com

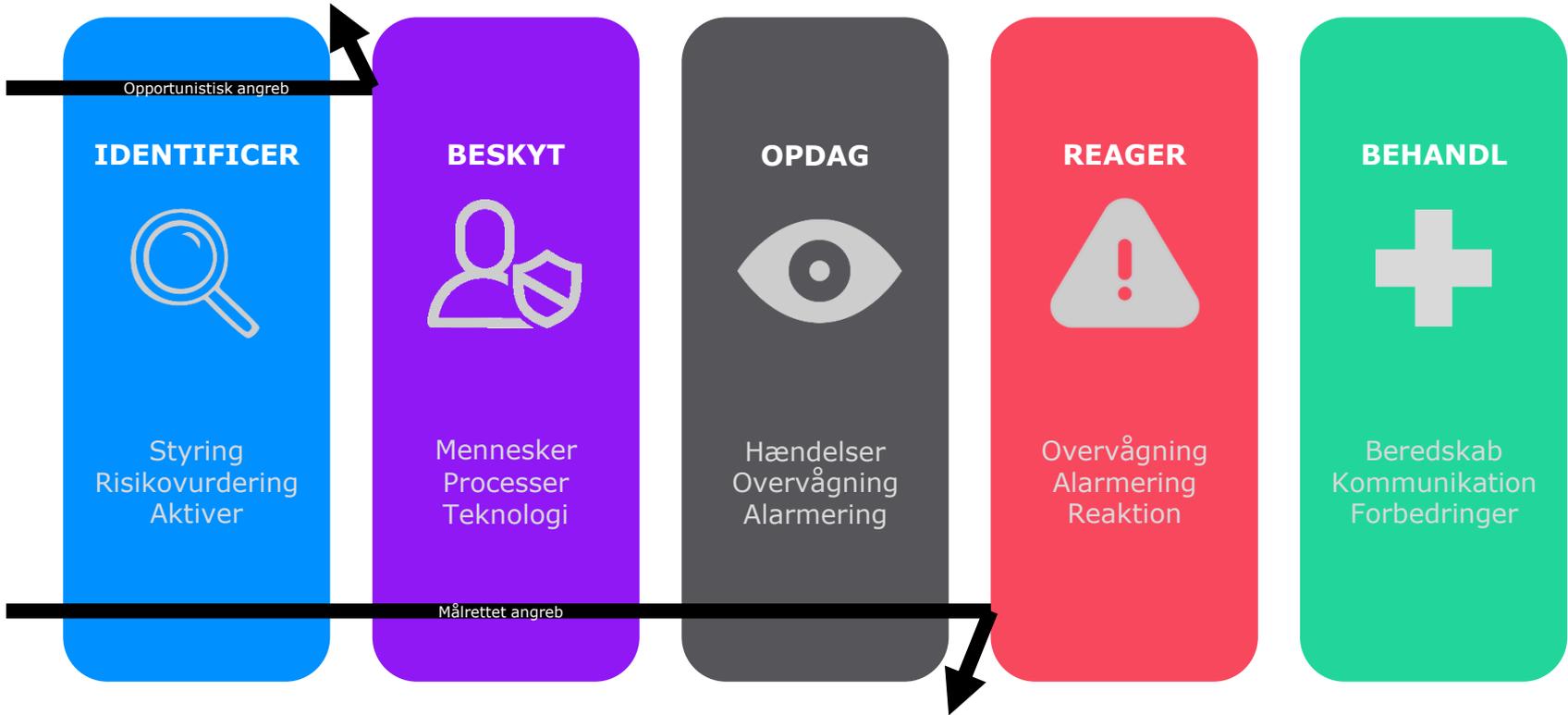
T : +45 4057 6828

Kaptajn, NBO Cyber
Samtækningssektionen
Operationsdivisionen





HVAD
GØR
VI?



Kilde: NIST Cybersecurity Framework



	Identify	Protect	Detect	Correct	Governance
RISK	<ul style="list-style-type: none"> - Pro activity - Shadow IT detection - Process Maturity 	<ul style="list-style-type: none"> - Security by design - Deep Security (server) - Data Loss Prevention (DLP - share of data) - Extended Web filtering - Next G Firewall - Cloud APP Security 	<ul style="list-style-type: none"> - Deep Discover Analytics - Data Leakage Detection 		<ul style="list-style-type: none"> - Maturity
	<ul style="list-style-type: none"> - Security Incidents and threats - Contract Management - Asset Management - Risk register roll out (only partly cyber) 	<ul style="list-style-type: none"> - 2 factor authentication - Advanced endpoint protection (Intrusion Prevention) - VPN from unmanaged devices removed - Exchange in the cloud - Improved patch management - Local Admin Rights Removed - Mobile Device Management 	<ul style="list-style-type: none"> - Enterprise Immune System (machine learning - advanced IDP) - Advance Threat analysis (use behavior) 	<ul style="list-style-type: none"> - Business continuity plan - Process Maturity 	<ul style="list-style-type: none"> - Vendor management - Risk Management
Managed	<ul style="list-style-type: none"> - Risk register tool - Solarwinds (network management) - AD user management incl. role & rights - SCCM (application distribution) - SCOM (server management) - License Management / SNOW 	<ul style="list-style-type: none"> - Web reputation (PC) - Patch Management - Secure remote access - Endpoint antirus & malware protection - Gateway Antivirus & malware protection - Network protection (Firewall) 	<ul style="list-style-type: none"> - Log inspection - Intrusion detection - Logging of network activity - Logging of incidents 	<ul style="list-style-type: none"> - Improved situation management (incident response) - New test of IT DRP - Updated IT Disaster Recovery Plan - Test of IT DRP - IT disaster recovery plan (preparation) 	<ul style="list-style-type: none"> - Digital Compliance & Security Officer - Training - Management of physical security - ICT Security Meetings (organisation) - Awareness folder - Policy Awareness Guidelines - IT Security Policies (rewrite)

1. Hvad vil du beskytte?
2. Hvor mange penge har du til sikkerhed?
3. Hvordan bruges de bedst?
4. Hvad vil du gøre når du bliver ramt?





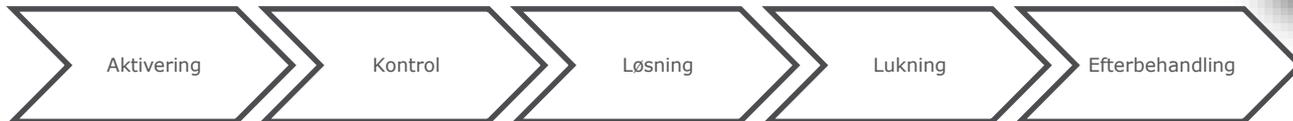
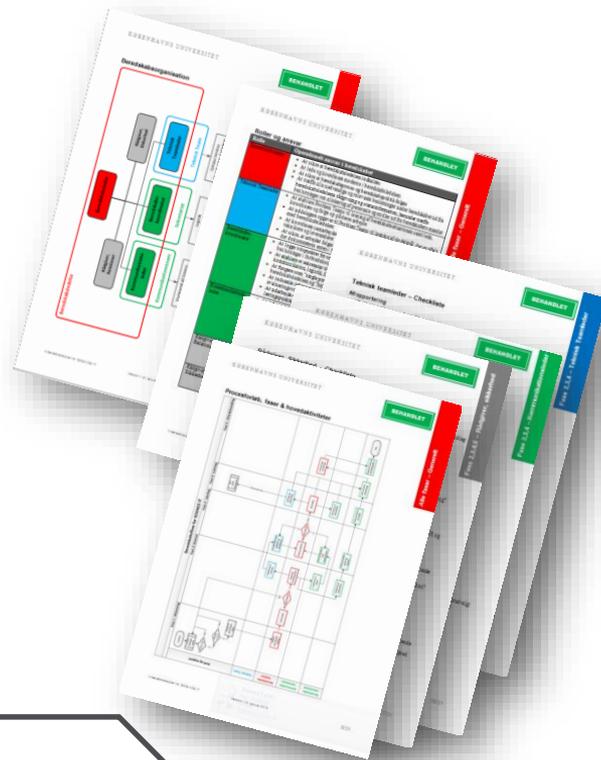
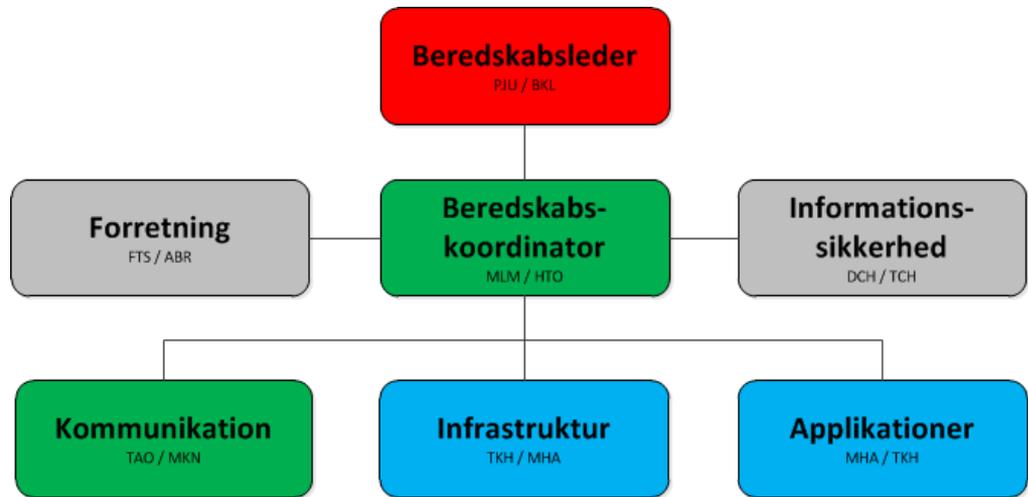
Akutmodtagelse

LADOMMEN

ERFARINGER SKABER CHECKLISTER

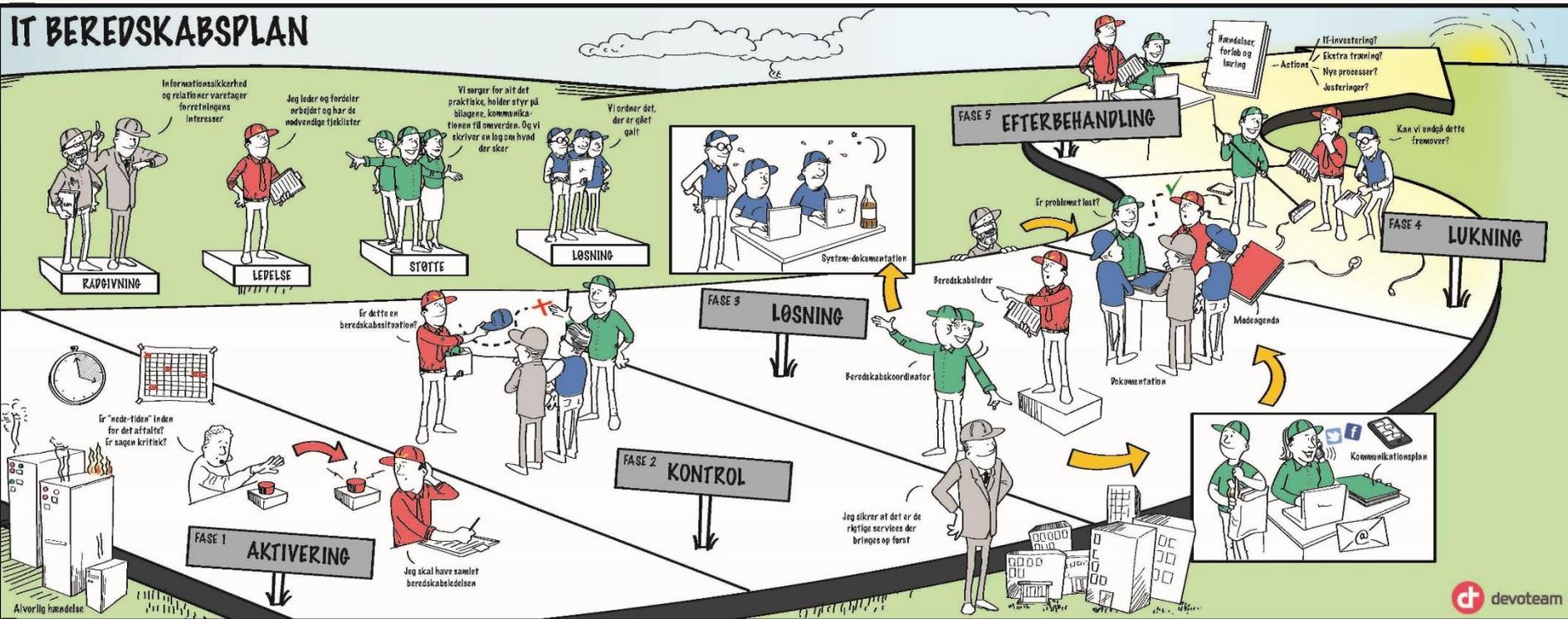
IT Beredskabsorganisationen

Struktur i kaos



Beredskabet - illustreret

IT BEREDSKABSPLAN



Action cards

Eksempel på agenda

Agenda – Startmøde i it-beredskabsledelsen

Deltagerkreds (konstituering)

- It-beredskabsleder
- Teknisk Koordinator
- Leverandøransvarlig
- Beredskabskoordinator
- Service Delivery
- Kommunikation
- Relationer
- Informationssikkerhed
- Andre? Nogle der mangler?

Status og situationsvurdering

- It-beredskabsleder går til tavlen og sikrer et samlet overblik
 - o Hvad er der sket og hvornår?
 - o Hvilke kritiske aktiviteter er påvirket?
 - o Hvad er teknisk status? (lav en liste over områder og problemer på whiteboard)
 - o Hvilke initiativer er allerede igangsat?
- Indkald relevante teknikere
- Skal der sikres beviser til myndigheder, forsikring eller en eventuel erstatningssag?

- Er det (stadig) en beredskabssituation, eller kan situationen håndteres af normal drift?

Planlægning og delegering

- Hvad skal opnås? Opstil og prioriter mål ud fra **kritikalitet**
- Hvem skal have ansvaret for løsning?
- Skal it-beredskabsledelsen indskrænkes/udvides?
- Opstil forslag til problemløsning (skal noget køres parallelt?)
 - o Nøddrift/**workarounds**
 - o Reetablering
 - o Root cause identifikation
- Beslut løsningsmodel og eventuelle alternativer (plan B, C etc.)
- Hvilke kriterier er der for skift af løsningsmodel? Hvornår går vi til plan B?
- Skal alternative løsningsmodeller forberedes?
- Opstil overordnet handlingsplan med delmål, tidshorisont og tidsestimater (whiteboard eller post-it)

Logistik og ressourcer

- Hvilke ressourcer skal allokeres?
- Hvad er mandskabssituationen? Kan der forudses ressourceproblemer?
- Skal ekstra personale varsles eller indkaldes?
- Skal eksterne ressourcer inddrages?
- Er der materiel, der skal anskaffes?
- Hvad er der mandat til i situationen (fx økonomisk råderum)?

Kommunikation

- Hvad er der allerede informeret om og til hvem?
- Hvem skal informeres og hvad skal der informeres om?
- Hvilke kommunikationskanaler skal anvendes?
- Opstil kommunikationsplan med opgaver og frekvens (whiteboard eller post-it)

Opsummering og mødeplanlægning

- Spørgsmål? Er alle klar over deres ansvar og opgaver?
- Vedtag tidspunkt for næste møde



PROBLEM
OWNER

KOMMUNIKATION
EKSTERN

BEREDSKABSLEDER

INFORMATION
SIKKERHED

SEKRETAR

Beredskabsvejledning

11.58.05

18:34

+5m

-5m

CALL

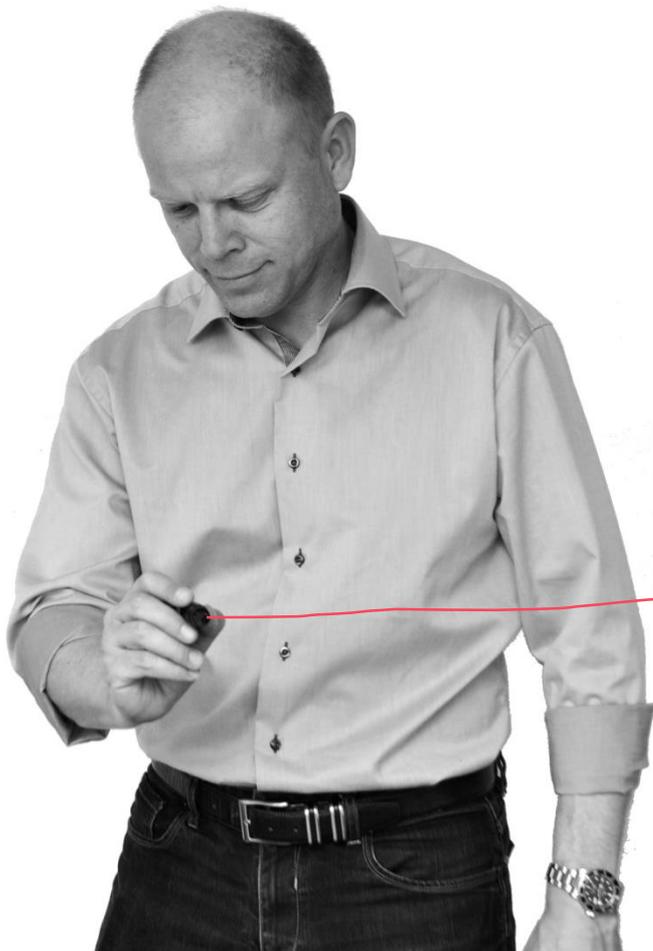
✓

⚒️



DU ER EN DEL AF DANMARKS CYBER FORSVAR





Frederik Helweg-Larsen

Expert Director, Risk & Security

fhl@devoteam.com

T : +45 4057 6828

Kaptajn, NBO Cyber
Samtækningssektionen
Operationsdivisionen