

pwc

Januar 2021

Seks strategiske temaer i en krisetid

Få gode råd og praktisk viden til håndtering af forretningsmæssige udfordringer

Revision. Skat. Rådgivning.

Indledning

Når en krise indtræffer, er det væsentligt, at en virksomhed reagerer hurtigt og rigtigt på de pludseligt opståede hændelser. Det kræver, at virksomheden er forberedt på og gearet til at håndtere den uforudsete situation for at sikre forretningskontinuitet og fortsat understøttelse af kerneopgaver og drift.

For at sikre forretningen i en krisetid er et opdateret kriseberedskab og en effektiv krisestyring i en organisation afgørende for, hvor modstandsdygtig denne er over for kriser.

Særligt under kriser, der har store udsving i omfang og konsekvens, som det fx gør sig gældende med COVID-19-krisen, spiller krisestyring en væsentlig rolle for at sikre virksomhedens fundament og overlevelse.

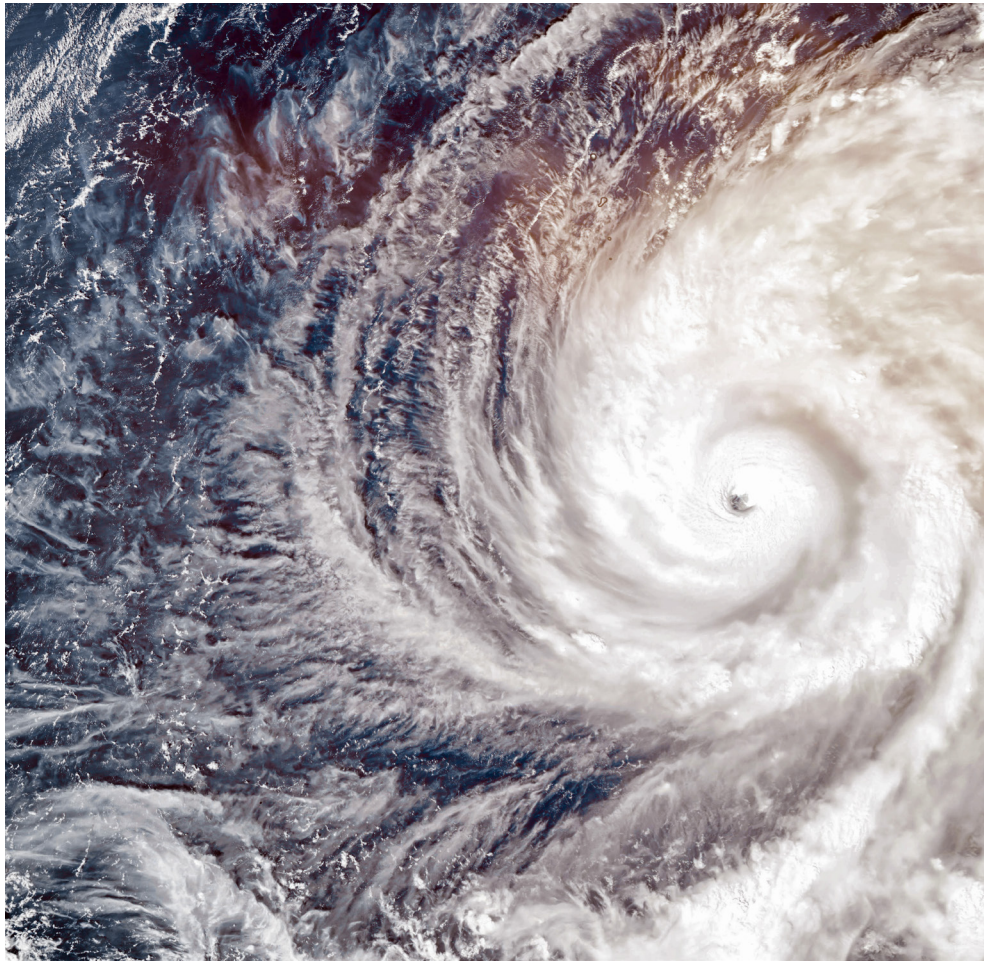
Formålet med effektiv krisestyring er blandt andet at:

- sikre indtægter og produktivitet i tilfælde af, at en uforudset hændelse indtræffer
- reducere omkostninger hvis en hændelse indtræffer på grund af hurtig eksekvering og mitigerende tiltag
- prioritere tiltag i forhold til sårbarheder og kritiske funktioner
- sikre en hurtigere tilbagevenden til "normalen"
- sikre organisationens omdømme og relationer til eksterne og interne interessenter
- opnå stærkere og bedre beslutningsgrundlag og deraf færre negative konsekvenser ved uforudsete hændelser og ændringer.

I det følgende stiller vi skarpt på nogle af de centrale forretningsmæssige udfordringer, virksomheder står overfor i en krisetid. Her får du praktisk viden og gode råd til, hvordan jeres virksomhed kan forberede jer på og gribe en krisesituation an, og hvordan der kan tænkes langsigtet for at komme bedst muligt ud på den anden side.

God læselyst!

Har du spørgsmål, er du naturligvis altid velkommen til at kontakte os. Du finder vores kontaktinformation bagerst i denne booklet.



Denne publikation udgør ikke og kan ikke erstatte professionel rådgivning. PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab påtager sig intet ansvar for tab, nogen måtte lide som følge af handlinger eller undladelser baseret på publikationens indhold, ligesom PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab ikke påtager sig ansvar for indholdsmæssige fejl og mangler. © 2020 PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab. Alle rettigheder forbeholdes. I dette dokument refererer "PwC" til PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, som er et medlemsfirma af PricewaterhouseCoopers International Limited, hvor hver enkelt virksomhed er en særskilt juridisk enhed

Indholdsfortegnelse



Likviditetsstyring i en krisetid
Få gode råd til at håndtere likviditets- og finansieringsudfordringer, når en krise indtræffer.



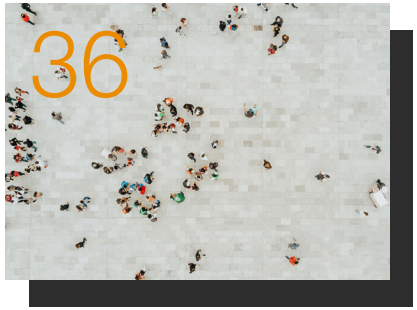
Fem trin til at få styr på omkostningerne
Få en illustration af en struktureret omkostningsreduktion gennem fem trin, og hvilke faldgruber du skal være opmærksom på.



Skab en robust supply chain
Få indblik i, hvilke kapabiliteter og digitale løsninger din virksomhed kan have særligt fokus på for at gøre din supply chain robust, stabil og transparent.



Risikostyring i en krisetid
Få gode råd til, hvordan din virksomhed kan identificere og strategisk håndtere væsentlige risici, der opstår i en krisesituation.



Forbered din organisation til fremtiden
Få indsigt i, hvordan man bør arbejde med sin kultur for at sikre, at den er gearet til fremtiden efter en krise.



Cyber Security-udfordringer i krisetider
Få gode råd til, hvordan ledelsen skal forberede virksomheden mod cybertrusler og håndtere trusselssituation i lyset af en krise.



Likviditetsstyring i en krisetid

Likviditetsstyring i en krisetid

Store globale kriser har ofte direkte indflydelse på markedsforhold. Således er størstedelen af danske virksomheder påvirket af de nye markedsforhold under COVID-19. Det kan skyldes en faldende aktivitet og dermed fald i indtjening, da omkostningsbasen er svær at reducere på meget kort sigt. Men det kan også skyldes, at virksomhederne ikke modtager betalinger fra kunder efter de aftalte betalingsbetingelser, eller at leverandører nu kræver kontantbetaling og ikke længere yder kredit. Alle disse forhold og mange andre har en direkte effekt på likviditeten og dermed også den finansiering, som er til rådighed for virksomheden.

I denne artikel får du et overblik over hvilke forhold, man som virksomhed især bør være opmærksom på i forhold til den afledte effekt af en krise på virksomhedens likviditet. Artiklen gennemgår forhold, som virksomheden skal have et overblik over på kort sigt samt hvilke initiativer, der kan igangsættes for at sikre, at virksomheden har det krævede likviditetsmæssige råderum til at kunne fortsætte driften. Desuden får du også gode råd til den interne og eksterne kommunikation samt hvilke forhold, man skal være opmærksom på i relation til ledelsesansvar. Endeligt giver artiklen dig indsigt i den praktiske udarbejdelse af et likviditetsforecast på kort og længere sigt.



Følgende emner gennemgås i artiklen

1 Forstå den nuværende finansielle situation

2 Beskyttelse af den finansielle situation

3 Håndtering af interne og eksterne interessenter

4 Likviditetsforecasting i praksis

5 Bestyrelsesmedlemmers ansvar

1. Forstå den nuværende finansielle situation

Når en krise indtræffer, er det nødvendigt at få et overblik over den disponible likviditet i virksomheden. Tiden, man har til rådighed til at få dette overblik, afhænger bl.a. af virksomhedens kompleksitet og branche samt de faciliteter, man har til rådighed.

Det bør undersøges om en del af virksomhedens likviditet er "trapped cash", som virksomheden ikke frit kan disponere over. Det kan fx være likviditet i et udenlandsk selskab, hvor man ikke har adgang til på kort sigt at disponere over likviditeten. Der kan også være likviditet, der er bundet på anden måde.

Vores anbefaling til at opnå forståelse af den likviditetsmæssige situation er at danne et overblik over følgende elementer:



Likviditetsberedskabet

De potentielle likviditetsmæssige konsekvenser af en krise bør vurderes både på kort og længere sigt med fokus på, om virksomheden har tilstrækkelig finansiering til rådighed. Dette overblik skal både bruges som et styringsværktøj, når likviditeten er knap, men også i den vigtige dialog som ofte opstår med banken i sådanne situationer. Det er vores erfaring, at man står i en væsentlig bedre forhandlingssituation med sine finansielle interessenter, hvis man er i stand til at kommunikere og fremvise et veldokumenteret likviditetsbehov.

Udgangspunktet bør være den tilgængelige eller frie likviditet, som ofte vil være summen af likvider og den kreditfacilitet, man har til rådighed hos virksomhedens bank, eller den andel heraf som ikke er trukket endnu.

Overvej følgende ved vurderingen af likviditetsberedskabet:

- Udarbejd og/eller gennemgå et kortsigtet likviditetsforecast for de kommende 13 uger – på dagsbasis eller ugebasis afhængig af den konkrete situation
- Opdatér forretningsplaner, budgetter og prognoser til den nye situation
- Identificér og dokumentér potentielle worst-case scenarier
- Udarbejd følsomhedsanalyse med modellering af worst-case scenarier og negative aspekter, inkl. indvirkningen af valutakursudsving
- Udarbejd og/eller gennemgå langsigtet likviditetsforecast for de kommende 12 måneder for at dokumentere turn-around planer for at vende tilbage til "business as usual".

Finansieringsfleksibilitet/kapacitet

Når der er dannet et overblik over likviditetsberedskabet, er det vigtigt at gennemgå relevant finansieringsdokumentation og identificere om et eventuelt yderligere likviditetsbehov kan understøttes af de nuværende låneaftaler, samt – i fald at det ikke kan - hvilke muligheder man har for at opnå yderligere finansiering.

Vi anbefaler, at virksomheder gennemgår og identificerer, om der er:

- Fleksibilitet hvad angår covenants, force majeure og baskets
- Yderligere lånekapacitet og ubehæftede aktiver, herunder eksempelvis varebeholdninger, tilgodehavender og IP-rettigheder
- Mulighed for at benytte regeringens hjælpepakker (som følge af COVID-19).

Beredskabsplaner

Vi anbefaler, at man udarbejder eller opdaterer sin beredskabsplan og identificerer hvilke håndtag, man kan trække i for at modvirke en forestående knap likviditet:

- Vurdér, hvor og på hvilket niveau, der om nødvendigt kan foretages faktisk omkostningsreduktion i fx medarbejderstaben, tilpasning af driftsaktiviteten til den lavere markedsaktivitet, udskydelse af investeringer mv.
- Vurdér, hvor og på hvilket niveau man kan omdanne hurtigt omsættelige aktiver i form af arbejdskapital til likviditet (reducere lagerbeholdninger, proaktivt inddrive overforfaldne tilgodehavender mv.).

Interessenthåndtering

Når likviditeten bliver knap, er vores erfaring at virksomheder oplever stigende forespørgsler fra deres interessenter, og de bliver derfor nødt til at dedikere ressourcer til at håndtere disse. Det er vigtigt, at man prioriterer dette, da et godt samarbejde med interessenter oftest er en forudsætning for at komme igennem en krisesituation.

Vi anbefaler derfor, at man danner sig et overblik over vigtige interessenter, herunder:

- Gennemgå kontrakter med vigtige leverandører og kunder – har man forpligtet sig til køb eller salgsvolumener, som man bør overveje at genforhandle?
- Undersøg kontraktmæssig fleksibilitet hvad angår ændring af betalings- og prisvilkår (for begge parter), og indgå i dialog med leverandører/kunder i forbindelse hermed
- Revurdér betalingsprioriteringer og overvej gældsafviklings-ordninger. Når likviditeten bliver knap, kan man stå i den situation, at man ikke kan indfri alle gældsforpligtelser, når de forfalder. Vi anbefaler en proaktiv dialog med kreditorer om mulighed for fx henstand eller afdragsordninger, hvis man ikke har mulighed for at betale gæld til tiden. Det er vigtigt, at huske ledelsesansvar i sådanne tilfælde, hvor man ikke må forfordele udvalgte kreditorer
- Overvej andre vigtige interessenters situation, fx aktionærer mv.
- Gennemgå forsikringspolicer med hensyn til klausuler vedrørende driftstab. Nogle virksomheder kan have tegnet en driftstabsforsikring, der kan dække dele af deres tab.



Det er vigtigt, at man prioriterer interessenthåndtering, da et godt samarbejde med interessenter oftest er en forudsætning for at komme igennem en krisesituation.

2. Beskyt den finansielle situation

Når der er opnået klarhed over den likviditetsmæssige situation, bør bestyrelsen og direktionen straks tage de nødvendige skridt for at sikre, at virksomheden som minimum kan opretholde denne situation, samtidig med at de identificerer muligheder for om nødvendigt at indhente yderligere finansiering eller likviditet.

Nedenfor er listet de foranstaltninger, som vi anbefaler, at man overvejer for at beskytte den finansielle situation i en krisetid. Om alle foranstaltninger er relevante vil afhænge af situationen samt virksomhedens størrelse, kompleksitet mv.



3. Håndtering af interne og eksterne interessenter

Håndtering af interessenter kan ofte være udfordrende i en presset situation, især hvor der er modstridende interesser, og der er et betydeligt behov for oplysninger i realtid.

Finansielle interessenter

Banker, obligationsindehavere, kreditvurderingsbureauer, revisorer

Driftsrelaterede interessenter

Udlejere, leverandører, kunder, kreditforsikringsselskaber, forsikringsselskaber

I forhold til sine eksterne interessenter anbefaler vi, at man foretager følgende handlinger:

- Identificér alle væsentlige eksterne interessenter; inddrag dem tidligt og sørg for proaktiv håndtering. I det omfang det efterspørges eller findes meningsfuldt, kan det være fordelagtigt at dele hele eller dele af de informationer, som er udarbejdet i forbindelse med virksomhedens forståelse af den finansielle situation. Dog er det vigtigt at være opmærksom på følsomme oplysninger.
- Forstå deres nuværende situation; gennemtænk hvordan eksterne interessenter eventuelt vil agere samt eventuelle forhold, der måtte opstå i relation hertil
- Vurdér indvirkningen af disse forhold på din forretning og arbejd sammen med interessenterne for at minimere eller afhjælpe indvirkningen.

I forhold til kommunikationsstrategi anbefaler vi, at man foretager følgende handlinger:

- Udarbejd en klar kommunikationsplan med henblik på at sikre konsistent kommunikation internt i organisationen såvel som eksternt til relevante relationer. Vores erfaring viser, at det er vigtigt, at virksomheden har en konsistent kommunikation udadtil, så leverandører, kunder og øvrige samarbejdspartnere ikke bliver forvirrede eller misinformerede over tvetydig information. Den interne kommunikation bør af samme årsag være konsistent og afstemt på tværs af organisationen
- Rådfør med jeres kommunikationsansvarlige eller udpeg eventuelt en til at varetage denne opgave.



4. Likviditetsforecasting i praksis

Et effektivt likviditetsforecast består af to hovedelementer, som er henholdsvis:

- Værktøjer
- Medarbejdere

Værktøjer (dvs. "hvad")

Et værktøj, der er tilgængeligt for hele organisationen

Kortsigtet likviditetsforecast, rullende på ugebasis for de kommende 13 uger efter den direkte metode ("cash-in / cash-out"-modellen)

Aldersfordelt debitorsaldoliste

Kladdefakturaer

Forventet salg, som endnu ikke er faktureret

Oprydning i "gamle" debitorer

Aldersfordelt kreditorsaldolistev

Nyt indkøb – købsfaktura er endnu ikke modtaget

Betaling af "gamle kreditorer"

Likviditetsforecast efter den direkte metode, Virksomhed ABC A/S

DKK i tusinde	Uge 1	Uge 2	Uge 3	Uge 4	Uge 5	Uge 6	Uge 7
Indbetalinger							
Indbetalinger	1.912	1.683	2.899	2.067	2.088	877	1.024
Ej faktureret salg	-	-	-	301	588	1.312	-
Nyt salg	-	-	-	-	1.050	1.000	-
Indbetaling af over-forfaldne debitorer	-	298	487	-	-	-	-
Indbetalinger i alt	**1.912**	**1.981**	**3.386**	**2.368**	**3.726**	**3.189**	**1.024**
Udbetalinger							
Kreditorbetalinger	(1.215)	(1.988)	(1.617)	(79)	(9)	-	-
Nyt køb	-	(420)	-	(446)	(2.395)	(2.634)	(1.267)
Løn inkl. A-skat	-	-	-	(4.800)	-	-	-
Moms	-	-	-	(1.941)	-	-	-
Betaling af over-forfaldne kreditorer	(1.941)	-	-	-	-	-	-
Udbetalinger i alt	**(3.158)**	**(2.408)**	**(1.617)**	**(7.266)**	**(2.404)**	**(2.634)**	**(1.267)**
Udvikling i likvider	**(1.244)**	**(427)**	**1.769**	**(4.898)**	**1.322**	**555**	**(243)**
Kassekredit, primo	**(10.645)**	**(11.889)**	**(12.316)**	**(10.547)**	**(15.445)**	**(14.123)**	**(13.568)**
Kassekredit, ultimo	**(11.889)**	**(12.316)**	**(10.547)**	**(15.445)**	**(14.123)**	**(13.568)**	**(13.811)**
Bevilliget kassekredit	**(15.000)**	**(15.000)**	**(15.000)**	**(15.000)**	**(15.000)**	**(15.000)**	**(15.000)**

Trækket på kassekreditten ved start af uge 1

Handlemuligheder?

Et effektivt likviditetsforecast består af to hovedelementer, som er henholdsvis:

- Værktøjer
- Medarbejdere

Værktøjer (dvs. "hvad")

Et værktøj, der er tilgængeligt for hele organisationen

Langsigtet likviditetsforecast, rullende på månedsbasis for de kommende 12 måneder efter den indirekte metode(beholdningsforskydnings-modellen)

Udgangspunkt er periodens resultat fra resultatopgørelsen

Ingen likviditetseffekt

Pengestrømme fra driftsaktivitet

Pengestrømme fra investeringsaktivitet

Pengestrømme fra finansieringsaktivitet

Samlet udvikling i likvider

Likviditetsforecast efter den indirekte metode, Virksomhed ABC A/S

DKK i tusinde	Måned 1	Måned 2	Måned 3
Periodens resultat	(3.795)	(7.286)	3.267
Finansielle omkostninger	(4.824)	(4.600)	(4.400)
Af- og nedskrivninger	3.947	4.000	4.000
Reguleringer i alt	(877)	(600)	(400)
Ændring i varebeholdninger	(384)	1.036	(1.345)
Ændring i tilgodehavender	(2.052)	(1.345)	(8)
Ændring i leverandører m.v.	980	(1.092)	(271)
Ændring i driftskapital	(1.456)	(1.401)	(1.624)
Pengestrømme fra drift før finansielle poster	**(6.128)**	**(9.287)**	**1.243**
Renteudbetalinger og lignende	4.824	4.600	4.400
Pengestrømme fra ordinær drift	**4.824**	**4.600**	**4.400**
Pengestrømme fra driftsaktivitet	**(1.304)**	**(4.687)**	**5.643**
Køb af materielle anlægsaktiver	-	(3.435)	(1.296)
Pengestrømme fra investeringsaktivitet	**-**	**(3.435)**	**(1.296)**
Tilbagebetaling af gæld til realkreditinstitutter	(1.156)	(1.200)	(1.200)
Kapitalindskud	10.000	-	-
Pengestrømme fra finansieringsaktivitet	**8.844**	**(1.200)**	**(1.200)**
Ændring i likvider	7.540	(9.322)	3.147
Likvider primo måneden	(14.074)	(6.534)	(15.856)
Likvider ultimo måneden	**(6.534)**	**(15.856)**	**(12.709)**

Likvider specificeres således:

Likvide beholdninger	1.347	486	411
Bankgæld	(7.881)	(16.342)	(13.120)
Likvider ultimo måneden	**(6.534)**	**(15.856)**	**(12.709)**

Handlemuligheder?

Dashboards til brug for rapportering og indsigt

Overblik over relevant output, herunder:

- Seneste forecast – detaljeringsgrad bør tilpasses slutbrugeren (bestyrelse vs. direktionen vs. afdelingsleder mv.). Salgsafdelingen kan finde en detaljeringsgrad på kundeniveau behjælpelig, mens bestyrelsen måske finder dette mindre vigtigt, men blot er interesseret i et overordnet overblik
- Forecast vs. forecast – hvad er ændret siden sidste forecast, og hvorfor? Det kan fx være en nedjustering af investeringer, der er blevet tilpasset i modellen, et tab af en kunde mv.
- Realiseret vs. forecast – variansanalyse på virksomhedens forecast sammenholdt med det realiserede likviditetstræk. Der bør indgå årsagsforklaringer. Dette er et vigtigt skridt til løbende at forbedre modellen – en afvigelse kan måske skyldes en vigtig post, som hidtil har været udeladt i modellen. Vores anbefaling er at følge op på ugebasis, og opfølgning bør være baseret på det faktiske træk på relevante banksaldi
- Forecastet likviditetsmæssigt råderum – opstår der knap likviditet de næste 13 uger eller 12 måneder? Vigtigt omdrejningspunkt til styring af likviditeten i krisetider, da det tillader virksomheden proaktivt at handle herefter
- "What if" scenarieanalyser på fx debitordage, fald i omsætning, tab af strategiske kunder, stigende råvarepriser, effekt af økonomisk støtte som fx hjælpepakker mv. for at stressteste likviditetspositionen – hvad kan virksomheden holde til inden for nuværende finansieringsrammer?
- Afstemning til salgsbudgetter, træk på varelager mv. for at kvalitetssikre modellens output
- Relevante kommentarer til output som følge af ovenstående punkter.

Det er vores erfaring, at det er en god øvelse at analysere de historiske pengestrømme for det seneste år eller to for at fastlægge, om der historisk har været sæsonudsving i virksomhedens likviditetstræk, samt identificere hvilke væsentlige poster, der påvirker likviditeten over året. Derved undgår man at overse poster, som fx ikke fremgår hyppigt (eksempelvis skattebetalinger, rentebetalinger, udbytter, kundebonus mv.)

Medarbejdere (dvs. "hvordan")

Ejerskab og ansvar uddelegeres

- Hvem leverer input og hvornår? Det er essentielt, at relevante parter inddrages i processen og forstår deres ansvar i den større proces, så der ikke opstår en flaskehals i opdateringsprocessen, fordi der mangler et væsentligt input
- Hvem ejer modellen? Det er vigtigt, at modelejeren afsætter den nødvendige tid til at vedligeholde og opdatere modellen. Ofte vil det være nødvendigt for vedkommende at overdrage hele eller dele af eksisterende arbejdsopgaver til en kollega for at frigøre den nødvendige tid. Herunder er det også vigtigt, at der etableres processer for overlap ved fx sygefravær og ferie
- Hvem modtager output og hvornår?
- Sæt faste ugentlige/månedlige deadlines for processen, som er afstemt med alle involverede parter.

Involvering af hele organisationen er vigtig

Udbred og understøt en likviditetskultur gennem åbenhed på tværs af organisationen fra indkøb til salg og supporterende funktioner som finans mv. Det er vigtigt, at det ikke blot bliver en tal-øvelse foretaget af finansafdelingen.

- Understøt en åbenhed om den likviditetsmæssige situation og synliggør konsekvenser af de valg, som tages fra indkøb til salg – det er vigtigt, at hele organisationen har en føling med dette, så der ikke foretages uhensigtsmæssige beslutninger, som påvirker likviditeten negativt, uden alle parter har været enige om dette. Det kan fx være i form af uhensigtsmæssige betalingsbetingelser for at vinde en kunde, pludselige forudbetalinger til en leverandør for at opnå prisrabat, fremskyndelse af ikke-essentielle investeringer mv.
- Når der er modtaget "buy-in" fra alle relevante parter i organisationen, sikrer man et retvisende og realistisk input/output
- Muliggøre at foretage relevante beslutninger på baggrund af en fælles opfattelse af virkeligheden.

Faktorer, der efter vores erfaring, ofte forhindrer et godt likviditetsforecast

- Modellen bliver for avanceret/tung at drifte
- Input/output er uoverskueligt, og udledning af vigtige konklusioner besværliggøres
- Der er en manglende koordinering/proces for indsamling af input og opdatering af model (deadline overholdes ikke mv.)
- Hele processen er forankret i finans uden inddragelse af den øvrige organisation
- Manglende opfølgning på forecasts
- Modellen glemmes i mellemliggende perioder, hvor likviditeten ikke er knap – tung proces at starte op igen.

Det er vigtigt, at det ikke blot bliver en tal-øvelse foretaget af finans-afdelingen.



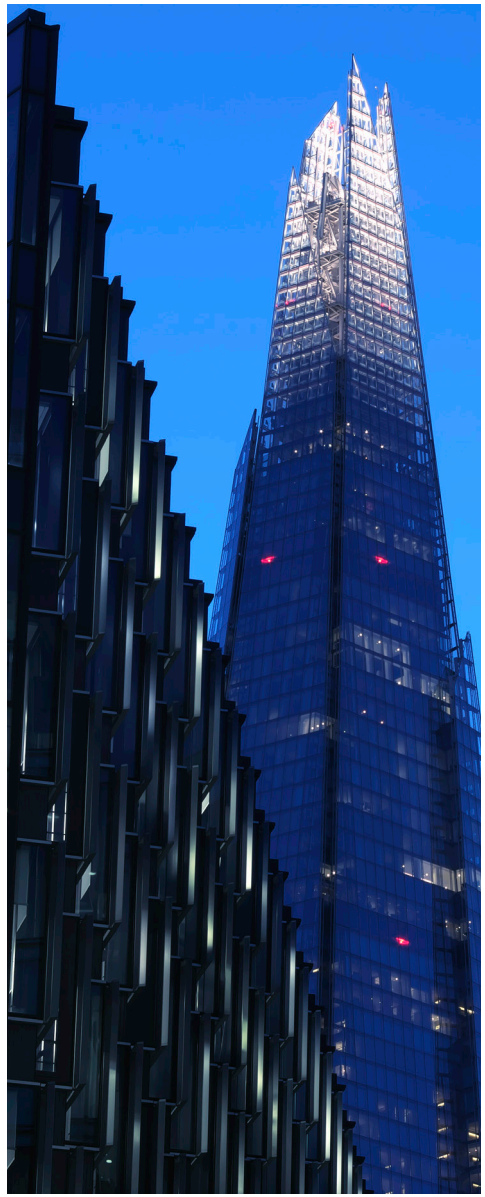
5. Bestyrelsesmedlemmers ansvar

I tilfælde af et finansierings- og likviditetsmæssigt pres skal bestyrelsesmedlemmerne flytte deres fokus væk fra aktionærerne og over til beskyttelse af kreditorernes interesser for at undgå uretmæssig drift.

Vi anbefaler, at bestyrelsesmedlemmerne gennemfører følgende trin

Indhent professionel rådgivning

1. Overvej virksomhedens finansielle stilling
   (se trin 1-3)
2. Vedligehold dokumentation for beslutningsprocessen
3. Overvej ophør af driften/going concern
4. Forøg hyppigheden af bestyrelsesmøder
   (evt. deltagelse i likviditetsmøder eller løbende opdatering om likviditetssituation)



Uretmæssig drift

Fortsættelse af driften på et tidspunkt, hvor der ikke er rimelig mulighed for at undgå konkurs eller rekonstruktion. Uretmæssig drift indebærer personligt ansvar for bestyrelsesmedlemmerne.



Omkostningsreduktion

Omkostningsreduktion

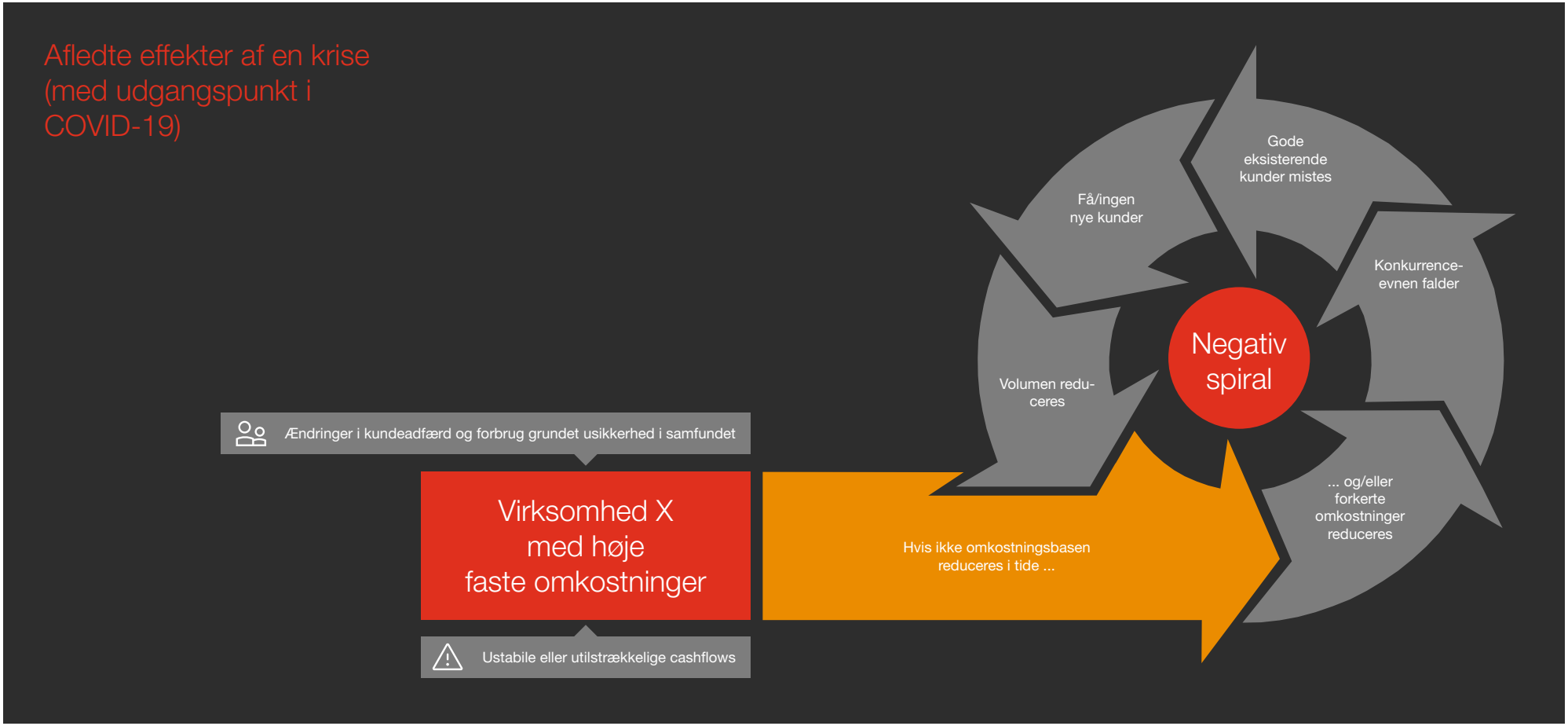
Hos PwC har vi en række anbefalinger til, hvordan I reducerer jeres omkostninger på kort sigt og tilpasser jeres forretningsmodel og driftsmodel efter en krise, hvis det er nødvendigt.

Baggrund

Når en økonomisk krise indtræffer, vil det være nødvendigt hurtigt at gennemføre omkostningsreduktioner for – i værste fald – at kunne overleve. Dette kræver indsigt i, hvor i virksomhedens værdikæde det er muligt at gennemtvinge omkostningsreduktioner.

Hastigheden, hvormed man får tilpasset virksomhedens omkostningsbase til en krisesituation, er afgørende, så en eventuel negativ spiral kan minimeres eller undgås. Det skal dog sikres, at tilpasningerne påvirker forretningsmodellen og virksomhedens konkurrenceevne mindst muligt.

I det følgende har vi gennem fem trin opstillet vores anbefalinger til, hvordan denne opgave bedst gribes an.



1. Overblik og nedbrydning af omkostningsbasen

For at fokusere indsatsen og opnå resultater hurtigt anbefales det at starte med at få skabt et overblik over virksomhedens forskellige typer af omkostninger og hvor i virksomheden, de er placeret.

Omkostningsbasen nedbrydes trinvist med afsæt i virksomhedens struktur og driftsmodel. Med denne tilgang er det muligt forholdsvist hurtigt at opdele omkostningsbasen overordnet i en række mindre omkostningspuljer med forskellige snit, fx løn, rejseomkostninger, ejendomsvedligeholdelse, projektomkostninger mv.

Typisk vil det allerede på dette stadie være muligt at identificere potentielle områder for omkostningsreduktioner (”quick wins”) og samtidig frasortere forretningskritiske områder, der i første omgang ikke skal være genstand for en dybere analyse.

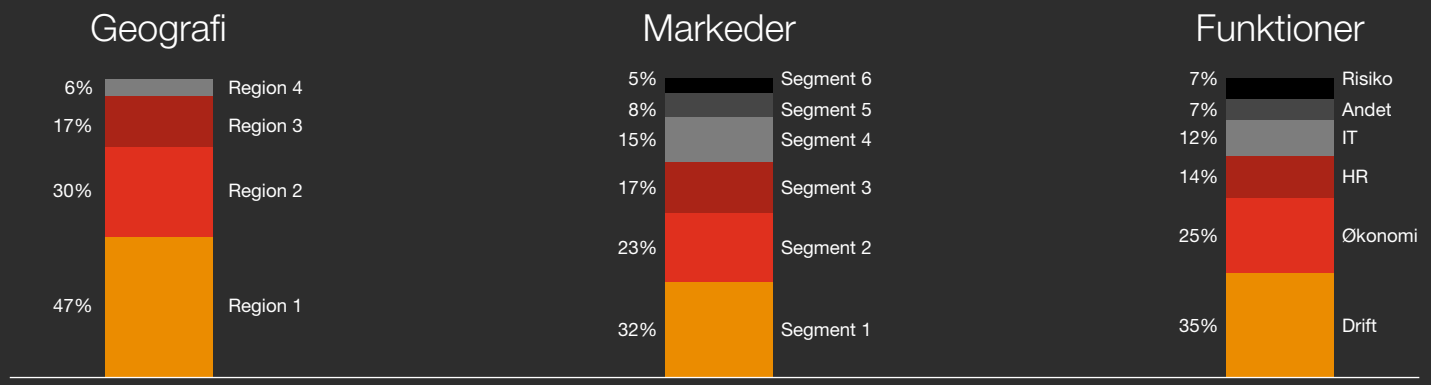
Nedbrydning af omkostningsbasen gør det muligt at fokusere arbejdet med at identificere og realisere omkostningsreduktioner mod områder med størst mulig effekt og samtidig med mindst mulig påvirkning af virksomhedens forretningsmodel og konkurrenceevne.

Nedbrydning af omkostningsbasen gør det muligt at fokusere arbejdet med at identificere og realisere omkostningsreduktioner mod områder med størst mulig effekt.

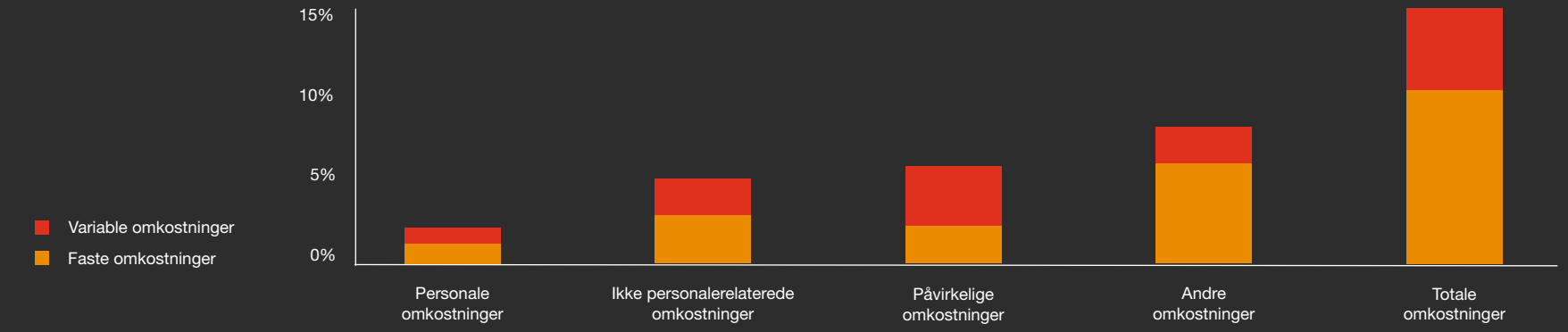


Eksempler på nedbrydning af organisationens omkostninger

Eksempel 1



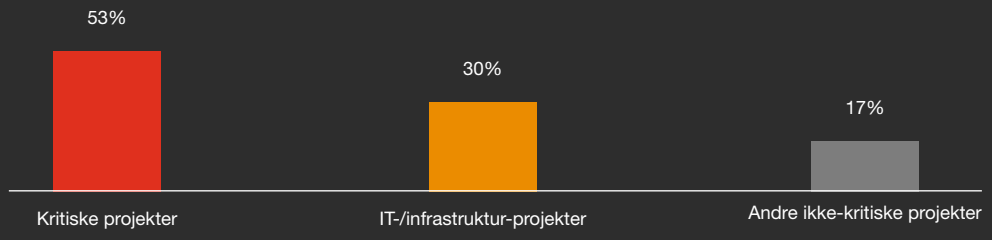
Eksempel 2



Eksempler på nedbrydning af organisationens omkostninger

Eksempel 3

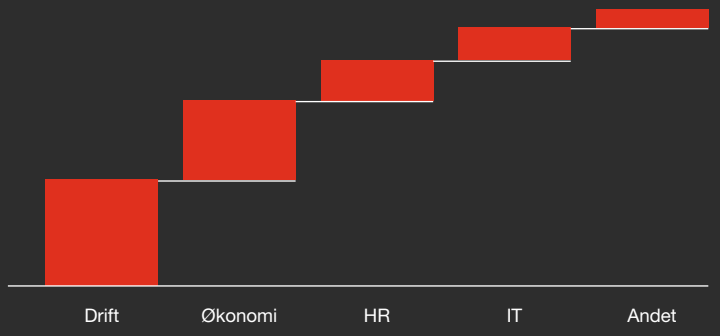
Projektomkostninger



Eksempel 4

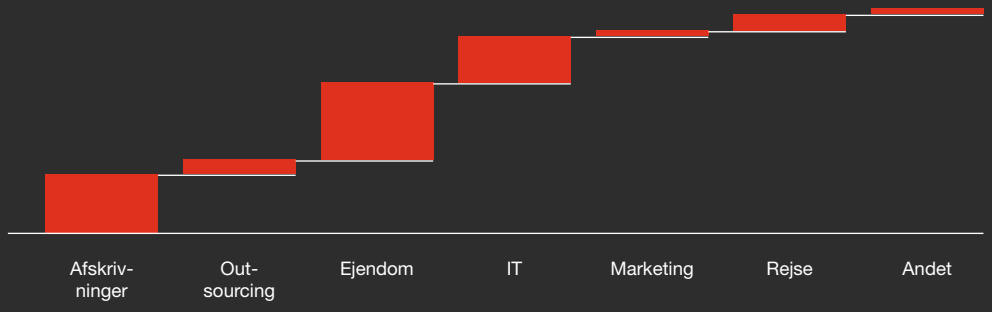
Personale-omkostninger

(FTE-reduktion gennem procesef-fektivitet - reducerede personale omkostninger gennem lønregulering og re-profilering)



Ikke-personale-relaterede omkostninger

(gennemgang af kristiske omkostninger til outsourcing, infrastruktur og ikke-kri-tiske omkostninger)



2. Kobling imellem omkostningsbasen og værdikæden

Ved at koble virksomhedens aktiviteter med omkostningsbasen skabes øget omkostningsgennemsigtighed. Dermed bliver det muligt på en datadreven og velovervejet måde at identificere muligheder for omkostningsreduktioner. Der bør her være fokus på at opdele omkostningsbasen i forhold til, hvor forretningskritiske omkostningerne er på kort sigt, samt i hvilken grad og med hvilken tidshorisont det er muligt at tilpasse de enkelte omkostninger til det aktuelle aktivitetsniveau.

1. Nedbrydning af værdikæden

Virksomhedens værdikæde nedbrydes i en række underliggende aktiviteter og projekter for hvert område.

Dette skaber indblik i, hvilke aktiviteter og projekter hele værdikæden består af. Når overblikket er etableret, påbegyndes koblingen af omkostningsbasen og aktiviteterne.

Virksomhedens værdikæde
(eksempel)



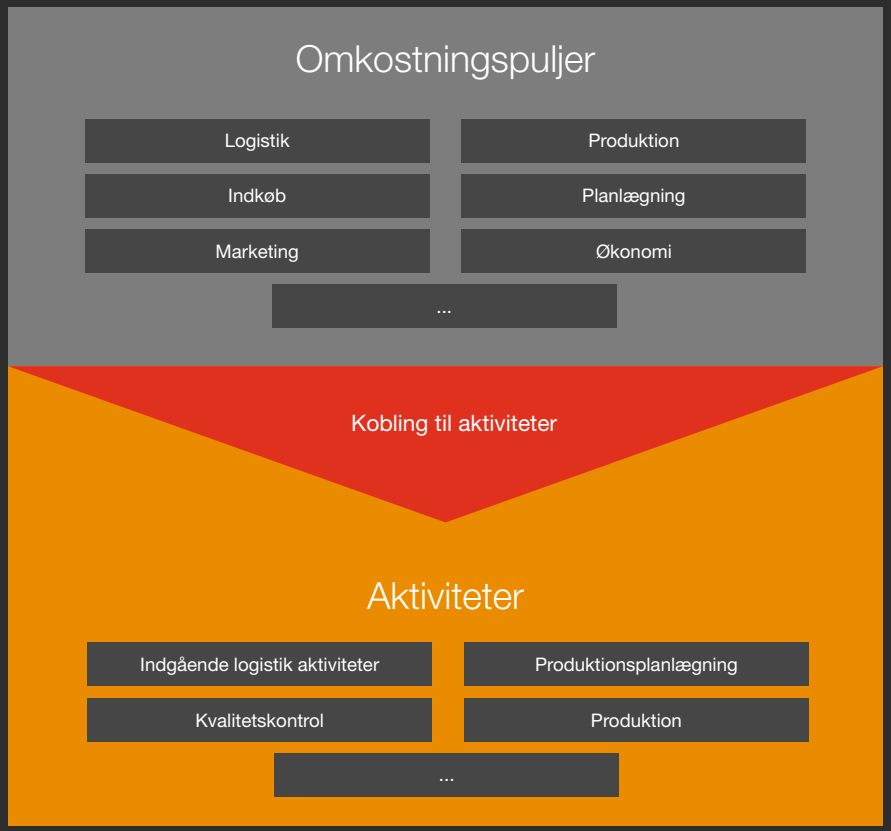
Ved at koble virksomhedens aktiviteter med omkostningsbasen skabes øget omkostningsgennemsigtighed.

2. Kobling af omkostningsbasen og aktiviteter

Hvis ikke omkostningsbasen allerede konteres med en struktur, der afspejler værdikæden og underliggende aktiviteter, skabes denne kobling i dette step.

Gennem overordnede fordelinger henføres omkostningerne til de identificerede aktiviteter og projekter.

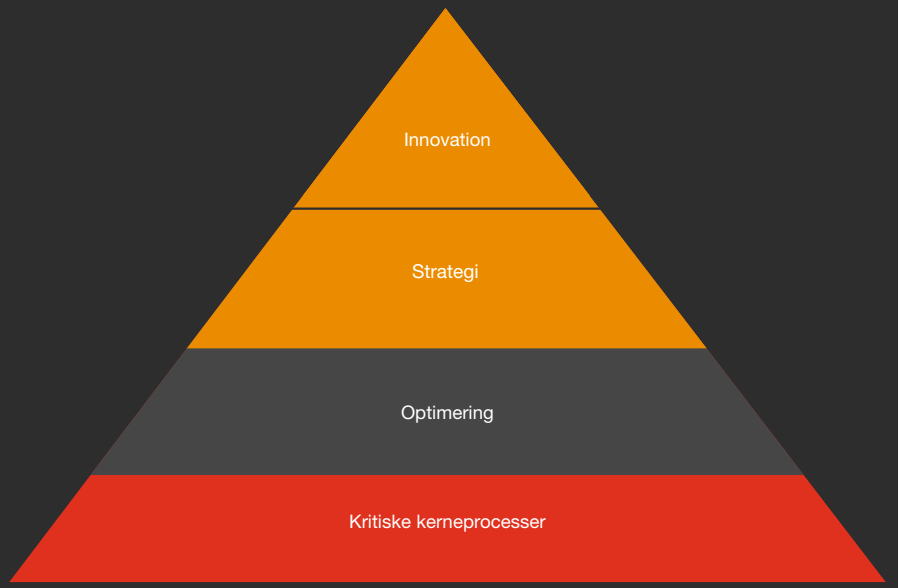
Kobling af omkostningspuljerne med aktiviteter



3. Kategorisering af omkostninger

Ved gennemførelsen af en omkostningsreduktion på kort sigt er det vigtigt at skære de "rigtige" omkostninger væk for at kunne bevare forretningsmodellen og konkurrenceevnen.

Vi anbefaler, at aktiviteter, projekter og tilhørende omkostninger kategoriseres ud fra nedenstående oversigt. Dette giver et overblik over, hvilke omkostninger der på kort sigt ikke kan skæres væk, uden at det påvirker forretningsmodellen og konkurrenceevnen.



Ikke-kritiske
Omkostning der er investering i fremtiden

Semi-kritiske
Omkostninger der skaber optimering, lavere risici eller øget compliance

Kritiske
Nødvendige omkostninger for fortsat drift

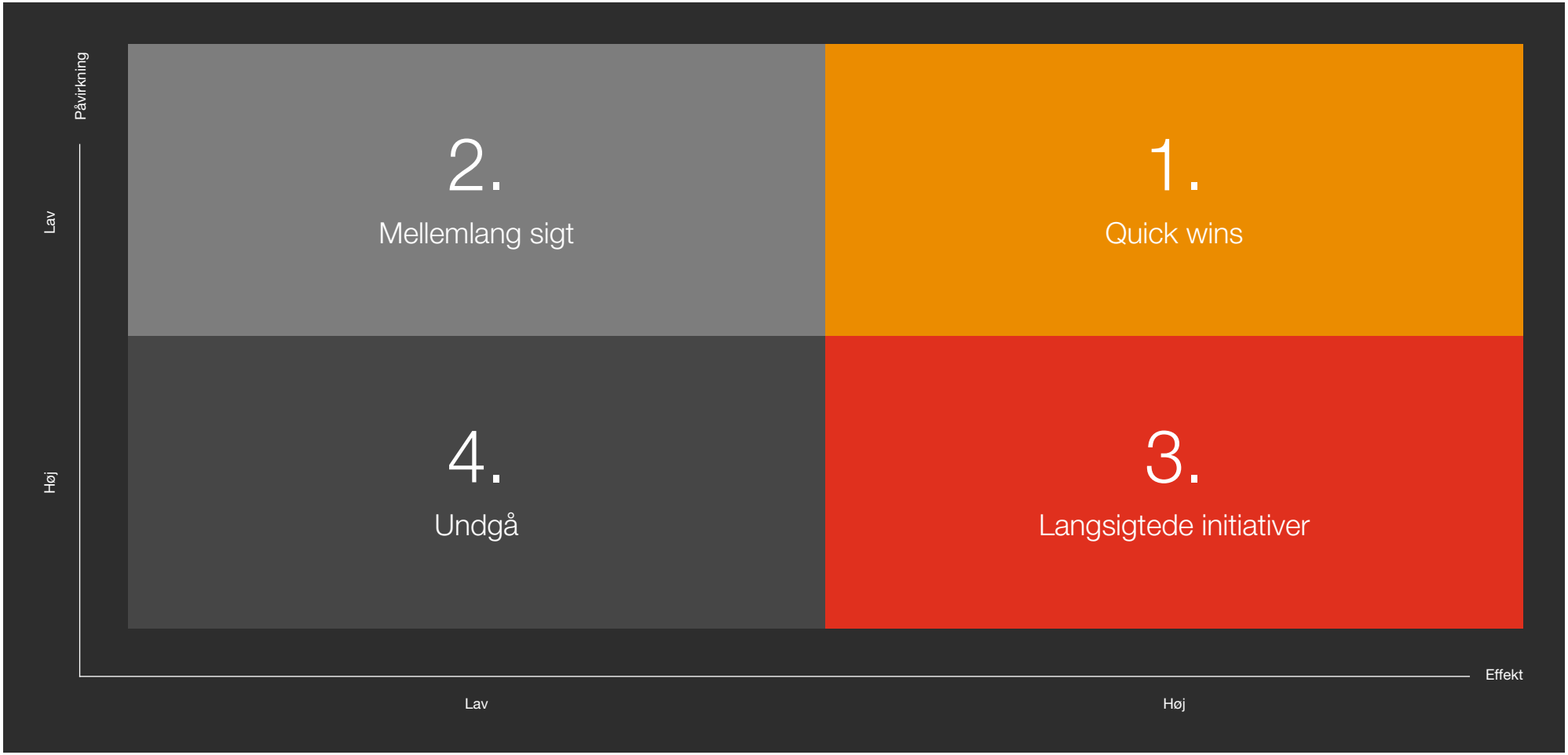
3 og 4. Eksekvering og løbende opfølgning

Sæt retning, vis lederskab og følg dernæst tæt op, og rapportér løbende på de enkelte initiativer – det er nøglen til succes for realisering af omkostningsreduktionen.

Ud fra den skabte sammenhæng mellem omkostningsbasen og aktiviteterne i step 2 kan virksomhedsledelsen i dette step udvælge og træffe beslutning om, hvilke omkostninger der kan skæres væk under hensyntagen til kritiske områder af virksomhedens værdikæde.

Det anbefales at lave en simpel og pragmatisk eksekveringsplan for hurtig gennemførelse af omkostningsreduktionerne.

De forskellige initiativer kan med fordel prioriteres ud fra nedenstående matrice. Det er vigtigt også at tage hensyn til eventuelle afhængigheder mellem initiativerne.





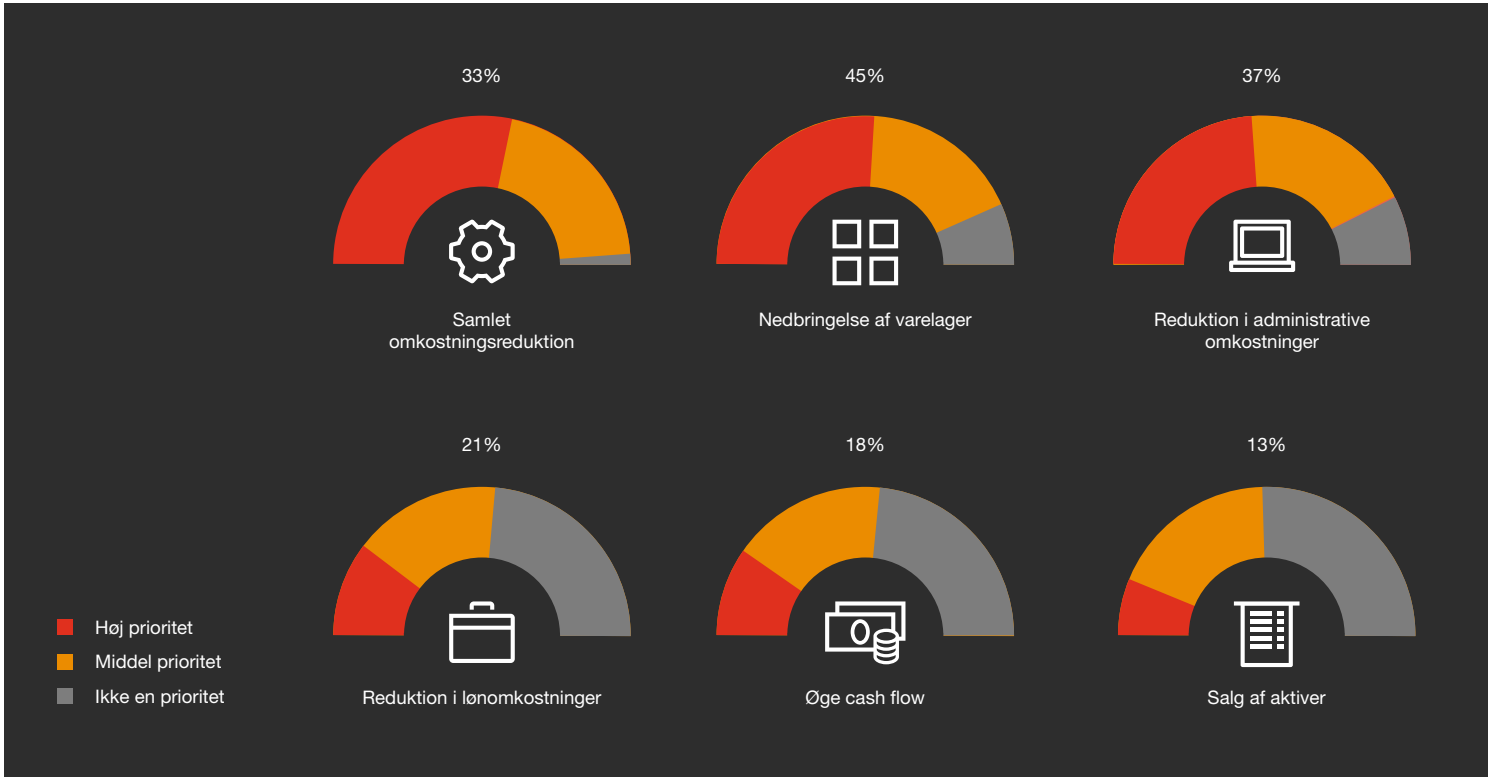
Omkostningsreduktion er en strategisk transformation af forretningen og kræver fuld opmærksomhed.

Det er vigtigt, at det drives som et strategisk initiativ med samme dedikation, retning og ansvarlighed fra bestyrelsen og/eller direktionen som ved andre strategisk vigtige initiativer.

Når omkostningsreduktionerne drives som et strategisk initiativ, sikres det bedste fundament for en effektiv operationel eksekvering.

Det gøres ved at sikre central styring, konsensus blandt den øverste ledelsesgruppe, engagement blandt medarbejdere på alle niveauer og at tilskynde personligt ejerskab og organisatorisk samarbejde:

1. Etablér en projektgruppe for at sikre, at den identificerede målsætning for omkostningsreduktionen bliver gennemført og besparelserne opnået til den aftalte tid.
2. Udarbejd en kort beskrivelse for hvert besparelsesinitiativ, der beskriver område, tidsrammen, estimeret besparelse og ansvarlige.
3. Etablér løbende rapportering og opfølgning på de enkelte initiativer.
4. Sikr rettidig kommunikation med de involverede interessenter.



5. Tiden umiddelbart efter krisen

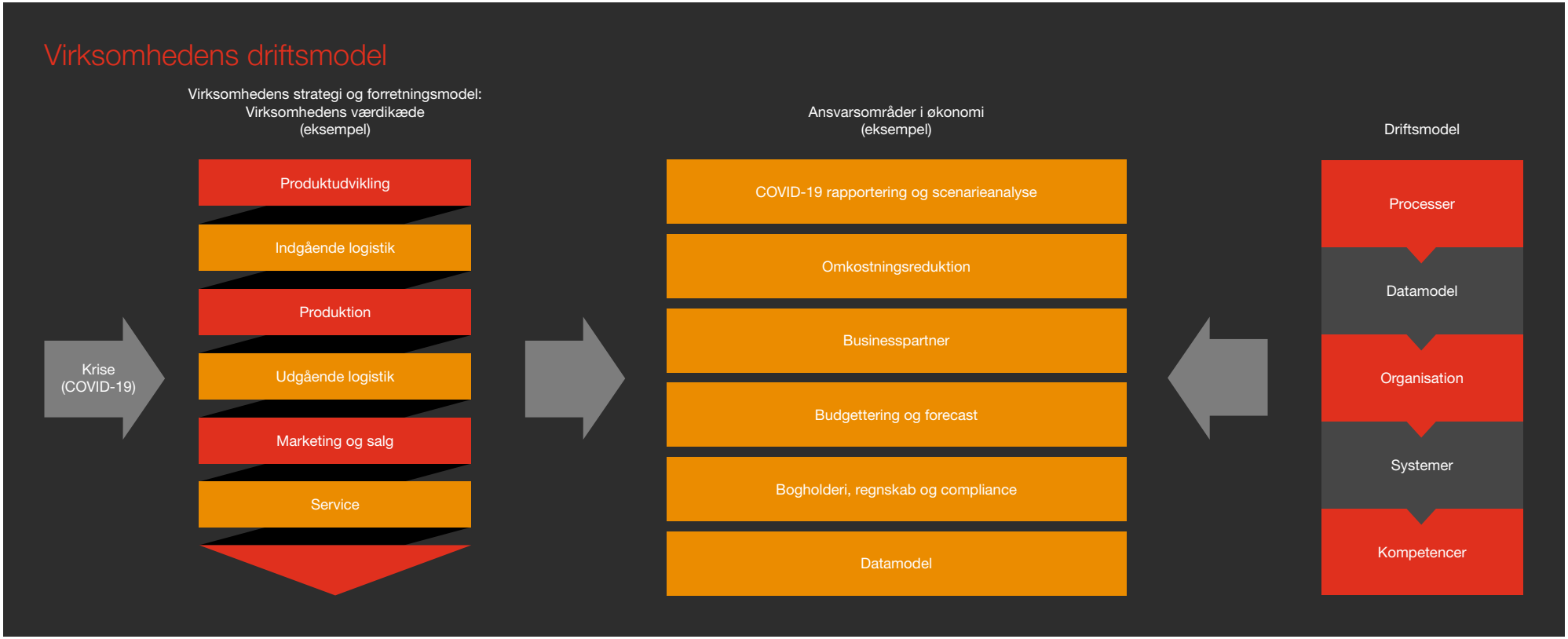
Det kan være nødvendigt at tilpasse virksomhedens driftsmodel til en ny situation efter efter en krise af betydelig karakter for virksomheden og forretningen. Vi anbefaler, at man allerede i forbindelse med omkostningsreduktioner overvejer og analyserer virksomhedens driftsmodel nærmere i forhold til organisering, kompetencer, normering, processer og systemunderstøttelse.

Når der er etableret en "normaliseret" driftssituation umiddelbart efter krisen, bør ledelsen kigge fremad. En nærmere analyse af virksomhedens konkurrenceevne, herunder udarbejdelse af forecasts og scenarier for den kommende periode (1-2 år), skal bibringe det fremadrettede fokus.

For nogle virksomheder kan det være nødvendigt at skære yderligere omkostninger væk for at sikre en sund og rentabel forretning. For disse virksomheder vil der være behov for at foretage justeringer i driftsmodellen. Det er her vigtigt at målrette virksomhedens ressourcer, hvor de kan give det bedste afkast i den nye situation, virksomheden befinder sig i.

Fokus bør være på at tilpasse de mere faste omkostninger til de forventninger, ledelsen har til aktiviteten på kort og mellemlangt sigt (1-2 år). Det er derfor vigtigt at analysere, hvorvidt virksomhedens organisering, ressourcer og kompetencer er afstemt til de forecasts/scenarier, ledelsen har udarbejdet.

Ligeledes kan det være nødvendigt at fremskynde investeringer, der kan effektivisere processer eller øge systemunderstøttelsen for at kunne blive mere konkurrencedygtig i en situation med dalene volumen.





Skab en robust supply chain

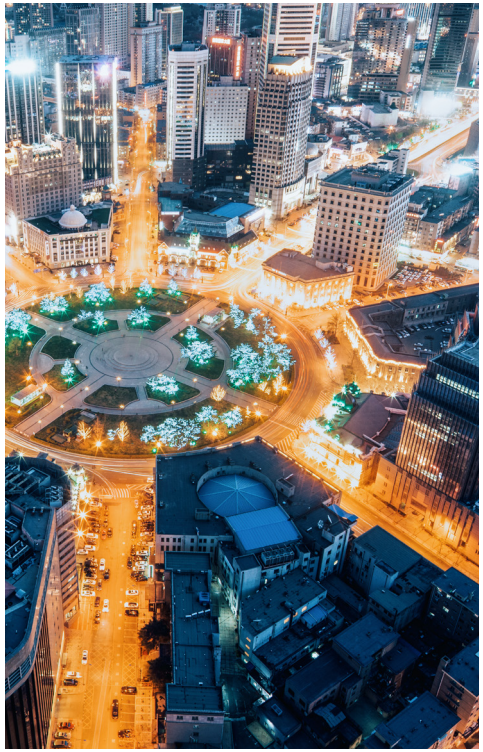
Skab en robust supply chain

Kriser stiller ofte virksomheder overfor en række store udfordringer i relation til deres leverandør- og forsyningskæders effektivitet og robusthed. COVID-19-krisen har fx medført store tilpasningskrav til virksomhederne og signifikante disruptions i form af uforudsete udsving i udbud og efterspørgsel, som har afsløret en sårbar supply chain i mange virksomheder. For at styrke virksomhedens supply chain er det aktuelt at se på, hvor robust strukturen i denne er, da det har direkte indflydelse på evnen til at håndtere risici og konstante forandringer i markeder. Alle led i virksomhedens værdikæde, hvor en mulig sårbarhed kan opstå, bør som følge af en krise ses i et nyt lys, da det er afgørende for, at virksomheden kan manøvrere midt i krisen og - mindst lige så vigtigt - at den hurtigst muligt er tilbage på benene igen.

I det følgende får du indblik i hvilke kapabiliteter og digitale løsninger, din virksomhed kan have særligt fokus på for at gøre din supply chain robust, stabil og transparent.

Supply chains bør ses i et nyt lys

Årtiers succesfulde udvikling af supply chain-planlægningsprocesser har skabt de supply chains, vi kender i dag. Understøttet af systemer og teknologier, der hele tiden bliver mere avancerede, er der nu skabt højt specialiserede og ikke mindst omkostningseffektive supply chains, hvor viden og erfaring er akkumuleret, og planlægning er løftet op på et højt aggregeret niveau på tværs af funktioner. Kriser som fx COVID-19 gør det nødvendigt ikke blot at se på, hvor omkostningseffektiv virksomhedens værdikæde er, men i særlig høj grad hvor robust den er. Særligt de mest produktive, teknologisk avancerede og videnstunge virksomheder, er også dem, der lige nu har den mest sårbare supply chain, og som bør gentænke de forskellige led i virksomhedens værdikæde.



"Mens fokus i mange år har været rettet mod optimering og omkostningsreduktion, har mange virksomheder i mindre grad fokuseret på balancen mellem effektivitet og robusthed. Vores forsyningskæder er blevet så omkostningseffektive, at vi har glemt, at de også skal være robuste."

Bo Dencker, partner hos PwC

Men hvordan skaber man en mere robust værdikæde? Det omfatter bl.a. tiltag som at indbygge buffere i form af flere ansatte og mere tid, at operere med større lagerbeholdninger, at øge gennemsigtigheden i alle led i værdikæden, samt at producere tættere på sine markeder. For at skabe og vedligeholde robuste forsyningskæder, peger PwC på vigtigheden af at se dette som en kerneopgave af strategisk karakter for den enkelte virksomhed. Supply chain-udvikling bør derfor være et emne, der bliver prioriteret højt på direktions- og bestyrelsesniveau.

PwC's eksperter anbefaler at skabe en robust supply chain gennem fire steps, som skal genbesøges i en årlig gentagende strategisk proces:



1. Forstå din forsyningskæde

Et forsyningssystem starter hos kunderne og ender hos leverandørerne – eller starter det hos leverandørerne og ender hos kunderne? Hvad enten man har den ene eller den anden approach, er det sikkert, at virksomhedens egen Operation skal være i stand til at kunne skabe den nødvendige fleksibilitet, som sikrer at kunde- og leverandørmarkedet hænger sammen.

Dette er en præmis for alle virksomheder.

Og erkendelsen af, at den enkelte virksomhed skal leve op til de forpligtigelser, den har pådraget sig i form af kontrakter indgået med kunder, er første step i forståelsen af virksomhedens forsyningskæde.

2. Re-design din forsyningskæde

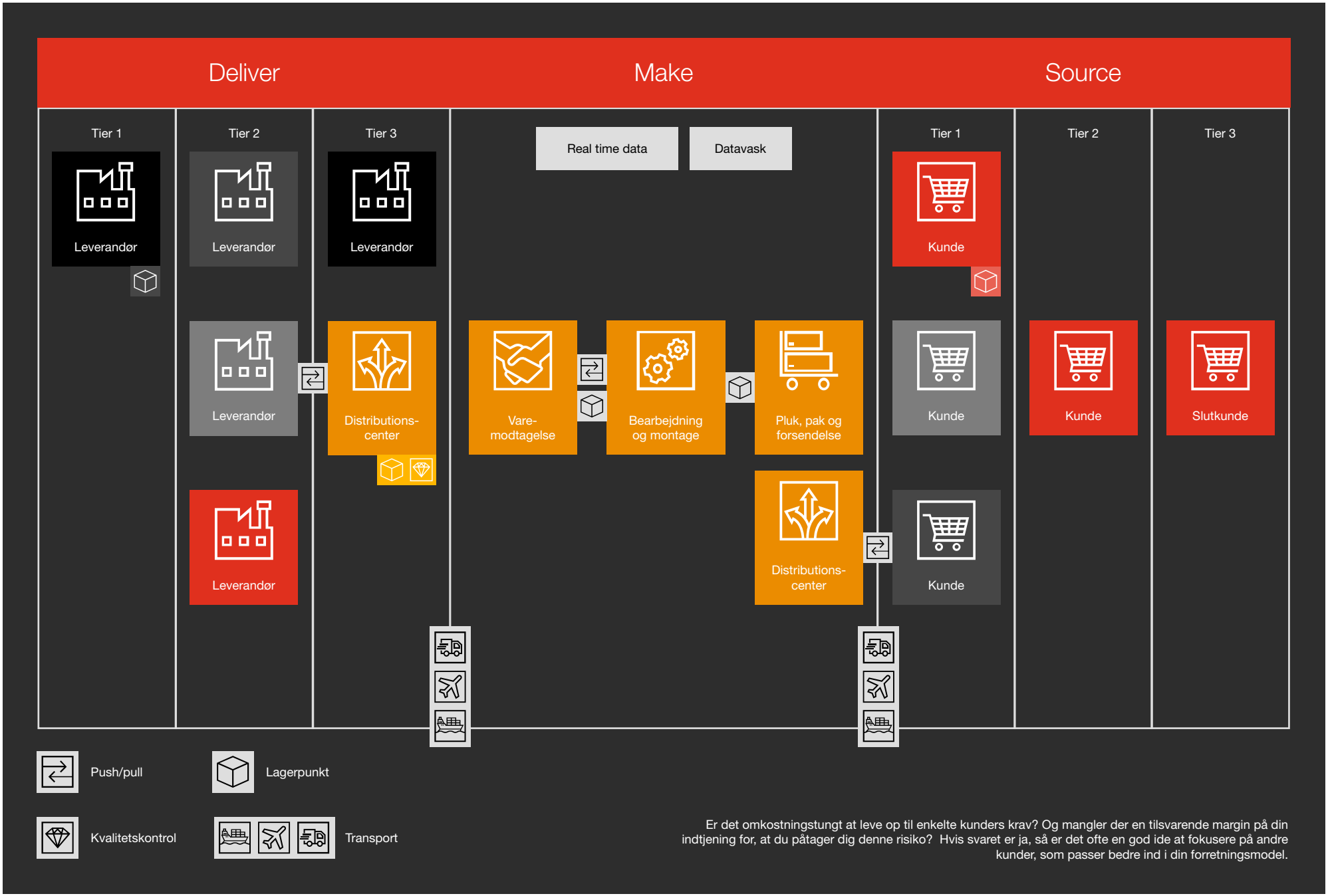
Næste step er forståelsen – og ikke mindst design af – hvordan den enkelte virksomhed sikrer sammenhæng end-to-end i værdikæden.

Den dobbelte segmentering af kunder og leverandører er et godt fundament for at skaffe sig en nødvendig fleksibilitet – simpelthen ved at tilbyde forskellige kunder og segmenter forskellige serviceniveauer. Og ved at opbygge processer og buffere afhængig af leverandør- og varegruppe.

Internt i egen Operation (produktion og distribution) skal der etableres et "styringskoncept", som med de rigtige lagerstørrelser og de rigtigt placerede push/pull-punkter i flowet sikrer den nødvendige fleksibilitet for at risikominimere de forpligtigelser, virksomheden har i relation til dens kunder.

Fordelen ved at integrere dette styringskoncept er, at virksomheden skaber sig et overblik over dels, hvad det koster i overkapacitet at supportere kundeforpligtigelserne, og dels hvilke kunder og hvilke leverandører, der forårsager specielt store risici i værdikæden.

Vi anbefaler alle virksomheder at arbejde strategisk med kunde- og leverancekæderne og sikre en spejling af kundekrav i designet af værdikæden. Se nedenstående illustration:



Er det omkostningstungt at leve op til enkelte kunders krav? Og mangler der en tilsvarende margin på din indtjening for, at du påtager dig denne risiko? Hvis svaret er ja, så er det ofte en god ide at fokusere på andre kunder, som passer bedre ind i din forretningsmodel.

3. Sørg for daglig ledelse af din værdikæde

Den daglige ledelse er det tredje element i opbygningen af en solid og robust supply chain. Alt for ofte sker det, at godt designede supply chains ikke er i stand til at leve op til de forpligtigelser, de har i form af leverancer til deres kunder eller i form af at skabe en sund bundlinje for virksomheden.

Årsagen til dette findes alt for ofte i, at ledelsen negligerer S&OP (sales & operation planning) – og at der derfor ikke er truffet "kloge tværorganisatoriske beslutninger" og udstukket rigtige retningslinjer, som grundlag for optimering af de mange beslutninger, der dagligt tages af en række medarbejdere i Operation.

Vi anbefaler derfor, at direktionen proaktivt deltager i S&OP-processen, således muligheder, risici og omkostninger løbende sikres afstemt. Man kan sammenligne med krisekommunikation, og hvordan ledelsen bør agere i forbindelse med krise- og risikostyring. Direkte involvering af direktionen og bestyrelsen bør også være til stede i udviklingen af supply chains for at skabe den optimale og nødvendige tilpasning af virksomhedens forsynings- og leverandørkæder.

4. Digitalisér din forsyningskæde

Det fjerde trin for sikring af den robuste supply chain er den digitale understøttelse. Det bliver stadigt mere vigtigt at have en elastisk supply chain med øget integration af data, hvilket giver et bedre overblik over, hvordan hele værdikæden fungerer, og hvor omkostningerne er placeret. De fleste virksomheder har et ERP-system (Enterprise Ressource Planning). ERP-løsningen kan håndtere alle de kerneprocesser, der er nødvendige for at drive virksomheden, således alle processerne er integreret i ét system samlet på ét sted. Men vi ser ofte, at ERP-systemet er middelmådigt implementeret – med risiko for fejlagtigt beslutningsgrundlag og deraf afledte fejlagtige beslutninger. Ligeledes ser vi ofte, at virksomhederne ikke udnytter en lang række muligheder for yderligere automatiseringer og for at skaffe og anvende data i realtid – både fra slutkunder, egen produktion og bagudrettet fra leverandørkæden.

Vi anbefaler en kortlægning af mulighederne for yderligere digitalisering og automatisering, således virksomheden hurtigt kan reagere og omstille sig – særligt i krisetider.

Strategisk fokus på robuste supply chains

Når man som virksomhed har fokus på de ovennævnte fire trin for at skabe og vedligeholde en robust supply chain, er det vigtigt at se design af supply chains som en strategisk kerneopgave for den enkelte virksomhed. Vi anbefaler derfor, at man som minimum én gang årligt bør genbesøge design af virksomhedens supply chain og opveje muligheder, risici og omkostninger, der ligger i dette design. I relation hertil er det væsentligt at udvikle kompetencer i virksomheden, der proaktivt afdækker risici og etablerer muligheder for at imødegå disse. Det er en opgave, der strækker sig på tværs af organisationen igennem hele værdikæden – og som også inkluderer udviklings- og finansfunktionen.

Gevinsten ved proaktivt at skabe den rette fleksibilitet og de rette, stærke partnerskaber i virksomhedens supply chain er evnen til at kunne agere agilt i en krisesituation, og derved at have energi til at opsøge de nye muligheder, der opstår som følge af ændrede markedskonditioner. Derfor er robusthed i supply chain blevet en konkurrenceparameter for virksomheder, der er afgørende for, hvor modstandsdygtige de er overfor kriser.





Risikostyring i en krisetid

Risikostyring i en krisetid

Effektiv risikostyring i en krisetid skal sikre:



En klar ansvarsfordeling omkring risikostyring – hvem gør hvad?



En opdateret risikoappetit og risikoprofil, som tager højde for ændringer i risikobilledet som følge af en krise



En effektiv og fokuseret forebyggelse af de rigtige og væsentligste risici



Løbende rapportering, der giver et retvisende billede af virksomhedens aktuelle eksponering



Robust opfølgning, der sikrer et beredskab overfor kendte såvel som ukendte risici.

Det er snart et årti siden, at den globale finanskrise tvang virksomheder til at tage en mere defensiv tilgang til risikostyring. Det betød, at mange virksomheder trak ansvaret tilbage fra forretningen til virksomhedens risikostyrings- og compliance-funktioner.

Det generelle risikolandskab har siden udviklet sig til et volatilt forretnings- og geopolitisk miljø med stadig mere sofistikeret teknologi og deraf følgende trusler. Hvilke risici, den enkelte virksomhed præcis er eksponeret for, afhænger af, hvilken industri, virksomheden opererer i, virksomhedsspecifikke forhold og ikke mindst virksomhedens strategi og globale udbredelse.

Risikoprofessionelle forsøger at forberede sig på alt, men få forestillede sig, at de skulle forberede modeller for en global krise, der rammer hurtigt og bredt og ikke har et klart sluttidspunkt, som det gør sig gældende ved COVID-19 krisen. Mens man så sent som i begyndelsen af 2020 særligt havde risikoscenarier som fx finansielle kriser, cyberangreb, risici omkring etik og ansvarlighed samt globale geopolitiske forhold højt på listen over mulige risici, var det imidlertid ikke mange, der havde detaljerede beredskabsplaner klar til at håndtere en global pandemi. Dette rejser et vigtigt spørgsmål: Hvordan tager man som virksomhed en mere proaktiv tilgang til risikostyring i en forandret verden, hvor man ikke kan forudse, hvad morgendagen bringer?

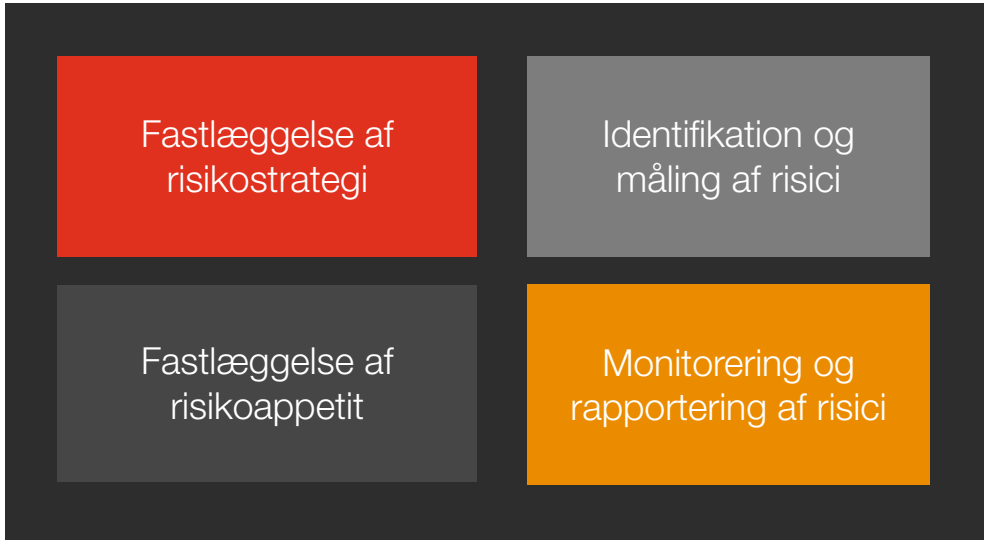
Nu, flere måneder efter COVID-19 brød ud, har samfund, borgere og erhvervsliv efterhånden nået en tilstand, hvor man lever med pandemien - en slags ny normal. Alligevel forventes fortsat en periode med store udsving og volatilitet i markeder og samfund. Byer og regioner over hele verden har været igennem flere bølger af pandemien, hvor restriktioner og retningslinjer skifter natten over, og hvor virksomheder løbende må tilpasse sig, mens forbrugere tilsvarende ændrer adfærd.

I kriser, hvor situationen indebærer mange ubekendte faktorer, er nøglen at have en fleksibel tilgang til forretningskontinuitet samt en bredere risikostyring. Men hvordan agerer man proaktivt snarere end reaktivt i en kontekst som denne? Det er i dag nødvendigt med en koordineret og integreret indsats på tværs af virksomheden, hvis man skal håndtere risici effektivt og sikre en profitabel vækst.

Risikoprofessionelle forsøger at forberede sig på alt.

Praktisk tilgang til risikostyring i en krisetid

Risikostyring er et redskab til bedre virksomhedsledelse, herunder at skabe et forbedret beslutningsgrundlag. Risikostyring skal ikke gøres til en teknisk disciplin. Det betyder, at ledelsen skal kunne omsætte strategi og forretningsmodel til risici – uden tekniske specialister. Vigtige delkomponenter i en robust og effektiv risikostyring inkluderer:





1. Fastlæggelse af risikostrategi

Risikostrategien danner rammeværket for virksomhedens styring af risici og indeholder elementer som målsætning, risikoappetit, organisering (inklusiv delegering af ansvar samt identifikation), måling, monitorering og rapportering af risici.

En klart defineret risikostrategi, der tydeligt kommunikerer virksomhedens holdning til risici, herunder hvilke risici, der styres og hvordan, vil understøtte en effektiv beslutningsproces og effektiv brug af virksomhedens ressourcer.

Der bør hertil implementeres en governance-struktur for, hvordan risikostrategien løbende revurderes. Fx om der er særlige situationer, der vil kræve revurdering af strategien, samt hvem der skal involveres. Der kan være tale om et fast forløb hvert kvarte, halve eller hele år, ligesom der herudover bør foretages en revurdering i forbindelse med væsentlige ændringer i virksomheden eller dens omgivelser som følge af eksempelvis globale kriser.

Bestyrelsen har ansvaret for at godkende virksomhedens risikostrategi, og det er derfor afgørende, at bestyrelsen har en forståelse for risikostrategiens enkelte elementer, samt hvordan disse påvirker hinanden.

2. Fastlæggelse af risikoappetit

Risikoappetitten er det samlede niveau for risiko, som en virksomhed er parat til at påtage sig for at realisere virksomhedens overordnede mål.

Risikoappetitten kan udtrykkes kvalitativt såvel som kvantitativt, hvor de kvalitative mål er mere overordnede og ikke udmelder en præcis grænse for, hvad der er acceptabelt. De kvantitative mål angiver derimod et præcist niveau for, hvad der er acceptabelt. Det betyder også, at disse er nemmere at monitorere og rapportere på.

Overvejelser, der ligger til grund for fastlæggelse af risikoappetitten, kan omfatte:

- Sammenhæng med risikostrategien, herunder områder hvor man er parat til at



acceptere en højere risiko, eller områder hvor man ikke ønsker at påtage sig nogen form for risiko
- Overvejelser om, hvorvidt virksomheden historisk har haft for restriktive eller for løse rammer for risiko
- Vurdering af virksomhedens modenhed inden for de områder, hvor man vil acceptere risiko.

3. Identifikation og måling af risici

Komitéen for god Selskabsledelse anbefaler i relation til risikostyring, at bestyrelsen årligt identificerer de væsentligste forretningsrelaterede risici, der knytter sig til virksomhedens strategi og mål, samt de risici, der har betydning for regnskabsaflæggelsen.

Identifikation og måling af risici foretages ved at indsamle oplysninger om virksomhedens risikoeksponering både i form af kvalitative og kvantitative data. Herefter opgøres målingen af risici, og dermed væsentligheden heraf, i henholdsvis hvilke konsekvenser de har for virksomheden, og hvor hyppigt de forventes at forekomme. Globale kriser, som fx COVID-19, medfører i mange tilfælde, at virksomhedens risikoeksponering ændres signifikant eksempelvis som følge af krisens konsekvenser for virksomheden, dens kunder og leverandørens økonomiske stilling, samt ændring i medarbejdernes tilgængelighed og evt. problemer i forsyningskæden.

Alle handlinger under kriser bør bygge på et solidt grundlag af viden. Informationer om risici er kritiske for langsigtet succes, men det gør sig ofte gældende, at der er begrænset information til at foretage forudsigelser. Gabet mellem den viden, virksomheden besidder, og vigtigheden af informationerne bliver dermed stort i forhold til normalt. For at indsamle den nødvendige viden til at kunne handle gælder det ikke kun om at se på den historiske udvikling. Her er det afgørende at lave fremadskuende beregninger og indsamle data om den forventede fremtidige udvikling. Især vil virksomheder, der forstår at forudsige kundernes adfærd og nye præferencer, være bedre stillede i krisetider. Informationerne skal ideelt ikke kun gælde for de næste måneder eller året ud. At få succes på kort sigt underbygger ikke altid den langsigtede strategi, og hurtige gevinster er ikke nødvendigvis relevante set i forhold til de velfunderede langsigtede formål.

4. Monitorering og rapportering af risici

For at bestyrelsen er i stand til løbende at foretage en vurdering af virksomhedens risici og tage beslutninger herom, anbefales direktionen løbende at holde bestyrelsen informeret om udviklingen på området.

Kommunikationsopgaven er vigtig, men ikke nem, og det anbefales, at bestyrelsen stiller krav til en enkel, relevant og rettidig rapportering, så vigtige risici ikke forsvinder i mængden.

Rapportering af risici kan fx ske kvartalsvist i tilknytning til den øvrige rapportering og kan indeholde:

- En simpel illustration, eksempelvis i form af et 'Risk map', der giver et overblik over virksomhedens væsentligste risici set i forhold til hinanden
- En simpel illustration, eksempelvis i form af et 'Risk map', der giver et overblik over

virksomhedens væsentligste risici set i forhold til hinanden
- En liste med virksomhedens top-10-risici, inklusiv handlingsplaner og ejerskab
- Et overblik over hvilke områder eller processer, der er mest eksponeret
- Aktuelle markedsforhold
- Ledelsens kortfattede analyse og vurdering.

Som supplement til monitorering og rapportering er de interne kontroller i virksomheden. Som et vigtigt led i risikostyringen skal de interne kontroller, som begrænser eller identificerer afvigelser fra vedtagne politikker og processer, designes og implementeres på en hensigtsmæssig måde.

Desuden anbefaler vi, at bestyrelsen aktivt udfordrer direktionen i forhold til den løbende monitorering og rapportering af risici.

Hovedparten af de store og mellemstore danske virksomheder arbejder i dag med risikostyring og har i den forbindelse etableret mere eller mindre formelle og veldokumenterede processer og procedurer for risikostyring. Globale kriser som COVID-19 giver dog anledning til en række vigtige overvejelser i relation hertil:

Seks vigtige risikostyringsovervejelser i forbindelse med COVID-19:

- Hvor og hvordan blev pandemisk risiko behandlet i forbindelse med de seneste risikovurderinger, og er der blevet gennemført en analyse af risiko relateret til interkonnektivitet eller samvarians for at forstå andre vigtige forretningsrisici, der er udløst af den pandemiske risiko?
- Udnyttes teknologiske værktøjer til konsolideret risikorapportering, herunder den hurtige udvikling i nøglerisikoindikatorer, der er specifikke for pandemisk risiko?
- Er der i lyset af COVID-19 behov for at gennemgå det foreliggende framework for risikoappetit med bestyrelsen og den øverste ledelse for at forstå den afledte effekt på virksomhedens aktuelle risikoprofil?
- Er ændringer i planer og procedurer kvalitetssikret af intern revision og/eller øvrige funktioner fra anden forsvarslinje for at sikre, at de afdækker pandemiske risikoelementer tilstrækkeligt?
- Hvilke forøgede risici skal adresseres (fx forøgede cyberrisici på grund af migration til hjemmearbejdspladser eller en tredjeparts ændrede processer som følge af pandemien), og er der etableret procedurer, som sikrer rapportering, aggregering og analyse af forøgede eller nye risici, i takt med at situationen ændrer sig?
- Hvordan vil COVID-19 påvirke din kontrolrapportering til dine interessenter - og din serviceorganisations kontrolrapportering til dig?



Sådan organiserer de bedste virksomheder deres risikostyring

Hvordan risikostyring skal forankres i virksomheden, og hvilke roller den enkelte afdeling skal udfylde, er væsentlige elementer i relation til beslutningen om organisering af risikostyring.

En praktisk og ofte anvendt måde at anskue forholdet mellem virksomhedens afdelinger på, er at betragte risikosystemet som tre 'forsvarslinjer', der giver en brugbar ramme for, hvordan forskellige afdelinger samarbejder.

'Første forsvarslinje'
udgøres af udførende ansatte i fx salg, indkøb og produktionsafdelinger, hvor afdelingerne har det primære ansvar for de risici, de påtager sig.

'Anden forsvarslinje'
er ansatte eller afdelinger, der er specialiserede inden for risikostyring, intern kontrol og compliance. Deres ansvar er at designe, koordinere og styre en konsekvent ramme og politik for at tage risici uden selv at være direkte eksponeret mod forretningsrisici.

'Tredje forsvarslinje'
udgøres af en uafhængig afdeling, eller en eventuel ekstern part, der løbende vurderer, hvorvidt virksomhedens risikostyringssystem er tilstrækkeligt, samt hvorvidt virksomheden efterlever de udstukne rammer for risikostyring.

PwC's årlige Risk Management-undersøgelse fra 2018 viser, at virksomheder, hvor ansvaret for risikostyring placeres i første forsvarslinje, har en bedre organisatorisk robusthed og profitabel vækst. I praksis betyder det, at den første forsvarslinje vurderer forretningsrisici og indarbejder risikostyring i både strategisk planlægning og taktisk udførelse. Desuden sikrer de, at de væsentligste risici håndteres på de rigtige tidspunkter i processen. Anden forsvarslinje samarbejder med første forsvarslinje og kontrollerer og giver sparring til optimering af risikostyringsprocesserne. Endelig giver den tredje forsvarslinje en uafhængig og objektiv vurdering af, hvorvidt første og anden forsvarslinjes risikostyringsaktiviteter er forsvarlige og effektive.

Risikosystemet som forsvarslinjer

Udarbejde en stærk, risikokultur-fokuseret begrebsramme
der begynder hos bestyrelsen og direktøren og gennemsyrer hele organisationen

Afstemme risikostyring med strategi på beslutningstagerplan
så første forsvarslinje kan forudse forretningsrisici, når taktiske prioriteringer fastlægges

Rekalibrere risikostyringsprogrammet på tværs af de tre forsvarslinjer
hvor første forsvarslinje tager beslutninger om forretningsrisici, den anden forsvarslinje monitorerer den første, og den tredje forsvarslinje indtager en supervisionsrolle

Implementere en klart defineret ramme for risikoappetit
på tværs af organisationen

Udvikle risikorapportering
der gør det muligt for ledelsen og bestyrelsen effektivt at varetage deres ansvar i forbindelse med risikostyring



Kilde: PwC's Risk in review: Managing risk from the front line, 6th Annual Study, April 2017

Guide til at flytte risikostyringen til første forsvarslinje



Der er i praksis stor forskel på, hvordan virksomheder griber risikostyring an. Dog giver vi i det følgende et bud på, hvordan bestyrelsen gennem fem trin kan skabe rammerne for en robust og effektiv risikostyring ved at flytte ansvaret for styring af risici til den første forsvarslinje.

1. Sæt ambitiøse og entydige mål, inklusiv fokus på risici

- Bestyrelsen og direktionen bør sætte entydige mål og udleve disse, ligesom de løbende bør overvåge og evaluere målene for at vurdere effektiviteten
- Direktionen bør sikre en performancekultur og incitamentsstyring i overensstemmelse med virksomhedens risikokultur
- Ledelsens bør kommunikere klare og konsistente meddelelser på tværs af virksomheden
- Risici bør indarbejdes i de daglige rutiner og i beslutningstagning.

2. Ensret risikostyringen med strategien på tidspunktet for beslutningstagningen

- Et klart overblik over virksomhedens strategi giver den første forsvarslinje en fælles vision om at tilpasse beslutninger og adfærd. Dette gør virksomheden i stand til at reagere hurtigere på risici og disruption
- Beslutningstagere bør integrere risikostyring i både strategisk planlægning og taktisk udførelse.

3. Justér risikostyringen på tværs af de tre forsvarslinjer

- For at sikre en optimal formåen bør den første forsvarslinje eje beslutningstagningen for risici. Den anden forsvarslinje bør så overvåge denne, og den tredje forsvarslinje bør foretage uafhængigt og objektivt tilsyn
- Tydelige rammer og snitflader mellem de tre forsvarslinjer bør identificeres og defineres for at gøre det muligt at koordinere roller og ansvar effektivt. Ledelsen kan dermed bedre definere risici og tildele dem på tværs af de tre forsvarslinjer. Desuden kan ledelsen sikre, at de styres på de rigtige steder
- Hver forsvarslinje bør tildeles de rette informationer og nødvendige ressourcer for at fungere effektivt.

4. Implementér en tydeligt defineret risikoappetit og et rammeværk på tværs af organisationen

- Definér de risici, som virksomheden er villig til at tage for at opnå sine ambitiøse mål; risici, der ikke kan tolereres; risici, der kan tolereres over en kortere periode – og risici, som er nødvendige, da de er forbundet med opnåelsen af strategien
- Udarbejd en fælles begrebsramme for risikostyring, som styrer processen for aggregering, monitorering og antagelsen af risici. Denne proces bør udnytte teknologi og dataanalyse så vidt muligt
- Risikoappetitten og rammeværket bør kommunikeres klart og tydeligt til beslutningstagere.

5. Udvikling af risikorapportering, som gør det muligt for direktionen og bestyrelsen effektivt at udføre deres risikostyringsansvar

- Forbedre datastyring og dataindsamlingsprocesser for at understøtte risikorapporteringen
- En robust proces for aggregering, monitorering og rapportering af risici er afgørende for at sikre, at beslutningstagningen sker inden for den fastsatte risikoappetit og tolerance
- Rapporterings- og monitoreringsprocesser bør overvåge risici og tilhørende risikostyringsaktiviteter regelmæssigt
- Virksomhedens væsentlige risici bør tildeles ejere, som er forpligtet til at udarbejde detaljerede, tidsbestemte risikohandlingsplaner.



Forbered din organisation til fremtiden

Forbered din organisation til fremtiden

Hvordan vil en krise som COVID-19 ændre vores organisationer, måder at arbejde på og vores kultur? I en krisetid er der ingen tvivl om, at en virksomhed må prioritere sikkerheden og sundheden for organisationen og dens medarbejdere. Der må træffes hurtige beslutninger, der giver umiddelbar aflastning. Men det er også vigtigt at tænke langsigtet og se ind i perioden efter krisen.

Kriser tvinger os til at re-evaluere, genoverveje og forandre. Har vi de rette kompetencer? Er vores adfærd, som vi ønsker den? Og på hvilke måder kan vi forbedre? Succes med at overkomme kriser afhænger af, at organisationen er gearet til at følge med. Det er den, når den har den rette viden, forståelse og adfærd. Det er dét, vi kalder organisatorisk awareness, og det er dét, der gør, at organisationen kan oversætte strategi til handling. I denne artikel sætter vi spot på, hvad virksomheder bør se efter, når de skal adressere organisationens kompetencer og kultur og på baggrund heraf beslutte, hvordan man bedst muligt bør arbejde med disse for at sikre, at den er gearet til fremtiden efter en krise.

I artiklen introducerer PwC's eksperter, hvordan virksomheder sikrer fundamentet og udviklingen af den ønskede kultur under og efter en krisetid. Du får indblik i, hvordan virksomheden opnår dette ved at opbygge den rette forståelse, viden og kompetencer i organisationen gennem målrettede trænings- og kulturprogrammer.

Du får samtidig inspiration og vejledning til, hvordan du kan måle pulsen på din organisation og sammensætte det helt rigtige awareness-indsats til at understøtte udviklingen af en kultur, der er forberedt til fremtiden efter krisen.



Kriser tvinger os til at re-evaluere, genoverveje og forandre.

En krise kan være den ultimative disrupter, der kalder på organisatorisk awareness og strategisk beredskab

Kriseberedskab
En krise som COVID-19 har ført store dele af virksomheder og organisationer verden over i kriseberedskab. I tillæg til de helbredsmæssige konsekvenser for samfundet, er der ligeledes alvorlige forretningsmæssige og økonomiske konsekvenser for virksomheder og for den globale økonomi.

Krisen kræver umiddelbar handling og kritiske beslutninger om omstrukturering og nedskalering for at tilpasse sig en ny virkelighed. Men det er samtidig vigtigt, at man i den hurtige, kritiske ageren reflekterer over, hvilke konsekvenser og betydninger de beslutninger og handlinger har for organisationen på lang sigt. Det er væsentligt, at reflektere over, hvordan man bedst forbereder sin organisation til fremtiden efter krisen.

Hvordan engagerer vi vores kultur og sikrer optimalt strategiskberedskab i en krisetid?

Kræver organisatorisk awareness
For at få succes med at geare sin virksomhed til fremtiden efter krisen kræver det, at man har den rette awareness i sin organisation. Helt konkret skal organisationen have den nødvendige viden, forståelse og adfærd, så den er tilpasset den nye virkelighed som følge af disruption. Men det bliver den ikke af sig selv. Det kræver, at ledelsen handler, mobiliserer kulturen og muliggør den nødvendige kompetenceudvikling.

Dilemmahåndtering – den komplekse ledelsesopgave
En krise som COVID-19 byder på klassiske såvel som nye dilemmaer. Her kan blandt andet nævnes dilemmaet om effektivitet vs. intimitet, individualitet vs. fællesskabet, kort vs. lang sigt, stabilitet vs. fleksibilitet og hastighed vs. koordinering. Det er en kompleks ledelsesopgave at navigere i de dilemmaer og finde den rette balance. Det kræver autentisk ledelse, der på én og samme tid tager højde for den enkelte medarbejder, samtidig med at svære og kritiske beslutninger skal træffes for at sikre virksomheden i en krisetid.

PwC's COVID-19 CFO Survey:
Virksomheder i kriseberedskab

76%

vurderer risikoen for en global recession som deres største bekymring.

56%

forventer at sende medarbejdere på orlov grundet lavere efterspørgsel.

49%

forventer at være nødt til at afskedige medarbejdere.

Kilde: PwC COVID-19 CFO Pulse Survey 2020

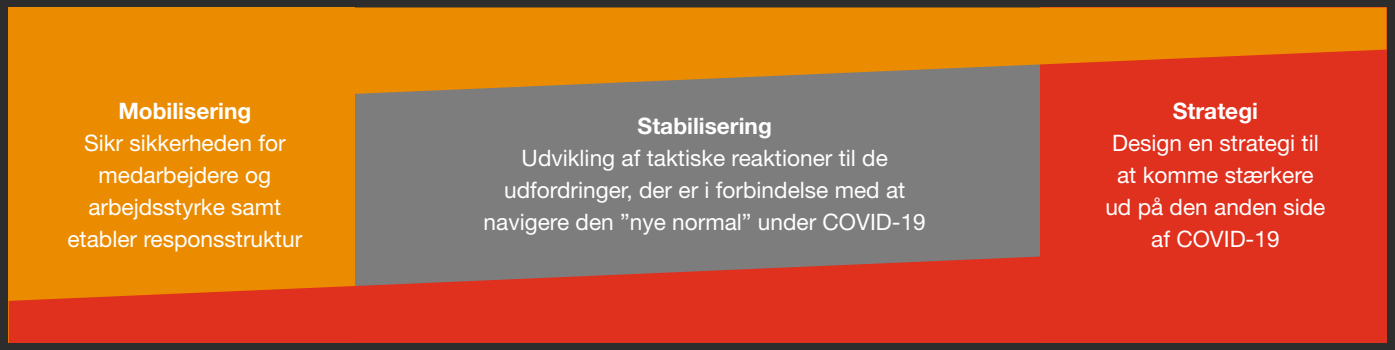
De handlinger, der foretages nu, vil tegne organisationer i lang tid fremover. Det kræver mere end akutledelse

Tænk strategi fra start og brug kulturen til at accelerere hastigheden

PwC har identificeret tre bølger af en kriserespons med udgangspunkt i COVID-19. Vores erfaring viser, at organisationer, der succesfuldt accelererer den hastighed, hvormed de kommer igennem bølgerne, har tendens til at komme stærkere ud på den anden side.

Der skal med andre ord tænkes strategisk fra start, og der skal være sammenhæng mellem virksomhedens værdier og kultur og de beslutninger, der træffes under de første to bølger.

Tre bølger af en COVID-19 kriserespons



Kilde: PwC 2020



Tre områder af særlig vigtighed i relation til COVID-19

PwC har identificeret tre områder, som vi vurderer er af særlig vigtighed for at fremtidssikre organisationer som følge af COVID-19.

1. Digital transformation

COVID-19 har tvunget mange virksomheder til at blive mere digitale meget hurtigt. Der er nye krav til, hvordan vi omgås, arbejder sammen, udvikler sammen, leder og følger sammen. For nogle handler det "kun" om nye kanaler og nye metoder. Andre ser ind i en større digital transformation og nye forretningsmodeller.

2. Upskilling

Allerede før COVID-19 var upskilling højt på agendaen i mange virksomheder. I lyset af COVID-19 bliver behovet for medarbejder- og kompetenceudvikling endnu mere væsentligt.

3. Kultur

Uanset virksomhedens udgangspunkt, dens strategi og respons til COVID-19, så bliver organisationens grundlæggende værdier og kultur rystet og testet, når man står overfor en krise af det omfang, som verden oplever lige nu.

Nogle virksomheder var allerede på en rejse, og har været testet mange gange før, fx. som følge af digital transformation eller øget regulering. For andre er det helt nyt - måske første gang - at man testes på kulturen.



Organisatorisk awareness binder det hele sammen

Kultur er anderledes end andre forretningsområder. Det er implicit fremfor eksplicit, og emotionelt fremfor rationelt. Det er det, der gør det udfordrende at arbejde med, men samtidig også så magtfuldt.

Effektive organisationer er dem, der formår at skabe sammenhæng mellem strategi, operating model og kultur. Derfor er kultur et vigtigt værktøj til at lykkes med virksomhedens vision og mission.

55%

er bekymrede for, at automatiske løsninger og/eller andre innovationer vil elimere deres arbejde.

Kilde: Edelman Trust Barometer 2019

60%

tror at kun få mennesker vil have stabile, langtidsvarende jobs i fremtiden.

Kilde: PwC Workforce of the future 2017

65%

ledere vurderer, at kultur er vigtigere end strategi og operating model.

Kilde: PwC Global Culture Survey 2018

I kriser er vi i ukendt farvand og har brug for et kompas. Mere end nogensinde har vi brug for kulturen

Succes vil i høj grad afhænge af, hvorvidt ledere formår at engagere deres organisationskultur. Hvordan gør man det? Ved at fokusere på dét, der virkelig betyder noget. Ved at identificere "de kritiske få".

Fokusér på de få, men kritiske komponenter, der for alvor kan accelerere virksomhedens kultur, fx den adfærd, I ønsker at fremme, og de nøglepersoner, der vil understøtte den ønskede adfærd i organisationen.

Særligt i en krisetid er det vigtigt at spørge sig selv: "Hvordan understøtter vores nuværende kultur de mål og intentioner, vi har, og hvordan får vi kulturen til at arbejde for og understøtte strategien?".

Aktivér din kultur ved at fokusere på de kritiske få, der har størst betydning, og brug kulturen til at accelerere strategisk sammenhæng og eksekvering.

Kulturelle træk
Identificér de væsentligste egenskaber, negative og positive, blandt den nuværende kultur.

Uformelle ledere
Lær fra uformelle ledere om, hvad de gør anderledes, der appellerer til og motiverer kollegaer.

Adfærd
Indstil fokus på tre eller fire typer af adfærd, der er tydelige, stærke og anerkendte.

Opfølgning
Definér parametre til at følge fremdrift med 'de kritiske få' og sæt retningen, der holder fokus på dette.

De vigtige spørgsmål, du bør stille dig selv som leder i en krisetid
Det er en kompleks ledelsesopgave at navigere i de dilemmaer og finde den rette balance. Det kræver autentisk ledelse, der på én og samme tid viser styrke og varme. Når den balance er rigtig, fremstår ledelsen autentisk, og der er en lige oplevelse af, at man passer på medarbejdere og har styrken til at sikre virksomheden i en krisetid.

1.

Varme og styrke: Hvilket signal sender din adfærd? Har dine medarbejdere en oplevelse af, at du passer på dem?

2.

De kritiske få: Har du identificeret og mobiliseret de kritiske få, der skal hjælpe dig med overgangen til en ny virkelighed? De skal kunne forstå og være i stand til at implementere dine beslutninger.

Hvordan understøtter vores nuværende kultur de mål og intentioner, vi har, og hvordan får vi kulturen til at arbejde for og understøtte strategien?



De handlinger, der foretages nu, vil tegne organisationer i lang tid fremover.

Opnå en stærk kultur og forbered din organisation til fremtiden gennem en målrettet awareness-indsats

Succes med at overkomme udfordringer afhænger af, at organisationen er gearet til at tilpasse sig dens kontekst. Det er den, når man har den rette awareness.

Men det kræver, at ledelsen handler og gør det muligt for organisationen og medarbejderne at skabe den nødvendige viden, forståelse og adfærd, der understøtter forretningsstrategien, virksomhedens operating model og den ønskede kultur.

Vores undersøgelser viser, at topledere er bekymrede for mangel på relevante kompetencer. Samtidig viser undersøgelser også, at arbejdsstyrken er klar til at lære nyt, men at de mangler at få muligheden for at lære. Et interessant dilemma, der understreger, at der et gab mellem gensidige forventninger og ageren. Kobler vi dette med den nuværende krise, vi står i som følge af COVID-19, er det vores vurdering, at behovet for organisatorisk awareness er yderligere accelereret.



Kilde: PwC CEO Survey 2019

Topledere er bekymrede for mangel på relevante kompetencer

79%

af topledere er bekymrede for tilgangen til relevante kompetencer. Det er en af deres top 3 bekymringer.

55%

af topledere siger, at mangel på kompetencer betyder, at de ikke kan innovere effektivt.

Arbejdsstyrken er klartil at lære nyt, menmangler muligheden

77%

siger, at de er klar til at lære nye kompetencer for at gøre sig relevante til fremtidens arbejdsmarked.

33%

kun en tredjedel siger, at de er givet mulighederne for at lære.

Kilde: PwC Hopes & Fears Survey 2019

Resultater og værdiskabelse med målrettet awareness-indsats



Hvordan sammensætter du den rigtige awareness-indsats til din organisation?

Det handler om at identificere den viden, kompetencer og erfaring, der vil være mest værdifuld i fremtiden for nye og ændrede roller, de individer, der kan levere i de roller og dertil udvikle en effektiv metode til at supportere og inspirere medarbejdere til at handle i dag og fortsætte med at tilpasse i fremtiden.

Det betyder, at man skal forstå gaps i viden og kompetencer, skabe den rette medarbejderoplevelse og sikre opbakning i hele organisationen, således at der frigives energi til forandring. Samtidig er det væsentligt at udvikle og implementere kompetenceudviklings- og kulturprogrammer, der sikrer den tilsigtede ROI (Return on Investment) ved brug af den rette indsigt og teknologier.



Fem centrale byggesten

1	2	3	4	5
Mål temperaturen i organisationen og identificér gaps	Byg en fremtidssikret kompetence-strategi	Identificér og mobilisér dine kritiske få	Design og implementér awareness program	Evaluér resultater og følg op på engagement
Forstå betydningen af disruption simplificering, regulering, digitalisering og automatisering	Få oversigt over og opdatér strategien for kompetenceudvikling	Identificér de væsentligste egenskaber, negativ og positive, af din nuværende kultur	Skab opbakning fra medarbejderne i organisationen	Følg op på resultater og målafkastning på investeringen
Definér fremtidig arbejdsstyrke og kapabiliteter (viden, kompetencer, processer, strukturer)	Sørg for sammenhæng mellem forretningsstrategi, operating model og kultur	Indstil fokus på tre eller fire typer af adfærd, der er tydelige, stærke og anerkendte	Skab tid og rum til læring og sørg for at sikre engagerende læringsoplevelser	Følg op på medarbejderengagement i organisationen
Undersøg nuværende kapabiliteter (viden, kompetencer, processer, strukturer) og identificér gaps	Optimér - hvis muligt - effektiviteten af HR-funktionen og -teknologien	Lær fra uformelle ledere, om hvad de gør anderledes, der appellerer og motiverer kollegaer	Byg digital forståelse i organisationen	Sørg for løbende aktivitet til at sikre forankring samt en struktur og format, der muliggør, at man kan tage ved læring af erfaringer undervejs
Kortlæg og engagér væsentlige interessenter og validér forandringsbehovet	Test strategiske alternativer og skalér de bedst performende programmer	Definér parametre til at følge fremdrift med de kritiske få og sæt retningen, der holder fokus på dette	Fokuser på målrettede medarbejderudviklings-rejser og levér træning	Benchmark kompetenceudviklings-organisationen (HR)

De vigtigste råd til at forberede organisationen til fremtiden

1. Tænk strategisk beredskab og organisatorisk awareness

- Kriser kalder på mere end bare akutledelse. Succesfulde virksomheder er dem, der hurtigt kommer igennem bølgerne, og det kræver strategisk handling fra start
- Disruption er ikke nyt. Det er nærmere en kæde af disruptere. Organisationen skal derfor konstant være forberedt på forandringer
- Succes med at overkomme disruption og udfordringer afhænger af, at organisationen er gearet til at følge med – selv i svære omstændigheder
- Det er den, når den har den rette viden, forståelse og adfærd. Det er dét, vi kalder organisatorisk awareness, og det er dét, der gør, at organisationen kan oversætte strategi til handling.

2. Identificér og mobilisér dine kritiske få

- Aktivér kulturen ved at fokusere på de kritiske få, der har størst betydning, og brug kulturen til at accelerere strategisk sammenhæng og eksekvering
- Sammenhæng mellem forretningsstrategi, operating model og kultur giver effektive organisationer. Organisatorisk awareness binder de tre elementer sammen
- Arbejd med den samlede organisation og kultur. Det er ikke en opgave for ledelsen alene.

3. Gør det muligt for din organisation at levere den tilsigtede værdi

- Mål temperaturen i organisationen og identificér den viden, forståelse og adfærd, der er nødvendig og vil skabe værdi for virksomheden i fremtiden efter en krise som COVID-19
- Muliggør kompetence- og kulturudvikling gennem en målrettet awareness indsats, der er relevant, engagerende og integreret
- Det behøver ikke at betyde store forandringer i grundlæggende processer og strukturer. Det er ikke dét, der er essensen her. Essensen er, at det handler om, at alle i organisationen skal være aware på virksomhedens strategiske retning. Og de skal have den nødvendige viden og kompetencer til at udøve den ønskede adfærd. Det er dét, der skal handles på.





Cyber Security-udfordringer i en krisetid

Cyber Security-udfordringer i en krisetid

I forbindelse med COVID-19 har mange virksomheder været og er fortsat udsat for cyber-angreb.Således har vi i 2020 oplevet det højeste antal sikkerhedshændelser i fire år, hvor hele 6 ud af 10 danske virksomheder har angivet, at deres virksomhed har været udsat for minimum én sikkerhedshændelse. Det viser PwC's Cybercrime Survey 2020. Undersøgelsen viser også, at 35 % af dem, der har været udsat for fx phishingangreb i 2020, at angrebet i nogen eller i høj grad har været relateret til COVID-19. Her kan der fx være tale om, at cyberkriminelle har benyttet COVID-19-relaterede budskaber i selve phishingmailen.

PwC's COVID-19 CFO Pulse Survey viser også, at danske økonomidirektører er reelt bekymrede for cybertruslen. Det forventes, at mange virksomheder vil opleve en negativ effekt på cybersikkerheden, bl.a. som følge af, at risici – eksisterende som nye – ikke adresseres i tilstrækkeligt omfang, fordi der skæres i sikkerhedsomkostningerne.

Ledelsens håndtering af cybertrusler og angreb er afgørende i en krisetid, og på de følgende sider får du gode råd og inspiration til hvilke ledelsesmæssige initiativer, man kan igangsætte for at højne cybersikkerheden.

En omlægning til hjemmearbejde og en samtidig øget prioritering af driftsmæssig kontinuitet medfører alt andet lige en række øgede risici:

- Sikkerhedskontroller i og omkring hastigt etablerede systemer og værktøjer, som understøtter hjemmearbejde og virtuelle møder, kan være fejlbehæftede eller helt fraværende. Det sker bl.a., hvis sikkerhedsteams ikke konsulteres vedrørende de nye systemer, før de tages i brug, eller hvis der tillades undtagelser fra sikringsaktiviteter, som normalt udføres. Dette fører til, at kontroller udelades, og muligheden for at opdage sikkerhedsbrud i disse systemer vil blive reduceret.
- Eksisterende processer og god praksis omgås eller er ikke tilgængelige for medarbejderne, når de pludselig arbejder på nye måder. Det kan fx være, at medarbejdere, der oplever, at deres normale sikre fildelingsmetode er uacceptabelt langsom, når de arbejder hjemmefra, vil ty til brug af gratis og ikke-autoriserede tjenester som et alternativ. Det kan desuden være, at medarbejderne ikke har adgang til sikker makulering af dokumenter derhjemme.
- Medarbejderne kan være mere udsat for social hacking, hvor de it-kriminelle benytter sig af medarbejdernes øgede arbejdsbyrde og uvante arbejdsmetoder. Der er allerede set phishing-angreb, hvor hackere har forsøgt at benytte sig af den potentielle uro omkring COVID-19. Udbredt hjemmearbejde vil få medarbejderne til at benytte sig mere af virtuel interaktion med kolleger, hvilket betyder, at den mere uformelle kommunikation og måder at bekræfte legitimiteten af dokumenter på sandsynligvis vil være mindre effektive.
- Afhængighed af adgangssystemer kan gøre virksomhederne mere sårbare over for overbelastningsangreb (DDoS). Opretholdelsen af pålidelige systemer til at styre adgang udefra for medarbejdere vil blive afgørende for forretningsdriften i takt med, at medarbejderne arbejder hjemmefra. Adgangssystemerne kan også blive mål for DDoS-angreb med henblik på at forårsage driftsforstyrrelser eller forsøg på pengeafpresning.
- Som følge af nye arbejdsforhold og -metoder vil mange medarbejdere være nødsaget til at arbejde med teknologier, som de ikke er fortrolige med, hvilket kan medføre, at der opstår nye sikkerhedsrisici. Mange medarbejdere vil skulle arbejde med uvant teknologi (fx online mødeplatforme) under et øget stressniveau, og med begrænset mulighed for tilstrækkelig oplæring. Det kan medføre nye risici, fordi teknologierne anvendes uhensigtsmæssigt, konfigureres forkert eller ikke anvendes med de sikkerhedsforanstaltninger, der oprindeligt var tiltænkt, og som er nødvendige for cybersikkerheden.

Medarbejderne kan være mere udsat for social hacking, hvor de it-kriminelle benytter sig af medarbejdernes øgede arbejdsbyrde og uvante arbejdsmetoder.

Den gennemgribende disruption, som krisen medfører hos medarbejdere og leverandører, vil også øge sårbarheden over for eksisterende risici:

- Der kan opstå sårbarheder, fordi grundlæggende sikkerhedsforanstaltninger som fx patching tilsidesættes, idet der sker en omprioritering af ressourcerne. Uanset de globale begivenheder opdages der fortsat sikkerhedssårbarheder i it-systemer, og det kræver en løbende indsats at sikre, at der reageres på dem, før it-kriminelle får mulighed for at udnytte dem. Hvis disse grundlæggende foranstaltninger tilsidesættes, vil sårbarhederne akkumuleres over tid med væsentligt øget risikoeksponering til følge.
- Virksomhederne opdager ikke cyber-angreb, fordi sikkerhedsteams er underbemandet eller er blevet om-allokeret til andre aktiviteter, og der derfor ikke følges op på sikkerhedsadvarsler. Sikkerheden via outsourcing-leverandører kan også være forringet som følge af serviceleverandørens udfordringer med egen arbejdsstyrke.
- Virksomheder kan have svært ved at reagere effektivt på cyber-angreb, fordi nøglemedarbejdere fra sikkerhedsafdelinger, it-leverandører og forretningen i bredere forstand ikke er tilgængelige og således ikke kan understøtte beslutningstagning og respons på et eventuelt angreb. Dette vil sandsynligvis især gælde virksomheder med lav modenhed, som er afhængige af nøglepersoner i stedet for at have fuldt dokumenterede og gennemprøvede processer.

De øgede cyber-risici som følge af COVID-19 rækker et godt stykke ind i fremtiden:

- Teknologier, der er blevet benyttet for bl.a. at understøtte hjemmearbejde, vil med stor sandsynlighed blive integreret i arbejdsmetoderne i virksomheden fremadrettet. Der er dog en risiko for, at disse teknologier i skyndingen med at få dem sat i drift ikke er blevet sikret i henhold til de samme sikkerhedsstandarder som andre it-værktøjer. Det kan fx være, at bærbare computere, der er sat hurtigt op til brug for hjemmearbejde, mangler væsentlige kontroller såsom fuld diskkryptering, hvilket gør de data, der opbevares på dem, sårbare, når arbejdsstyrken bliver mobil igen.
- Hjemmearbejde på kort til mellemlangt sigt vil dermed føre til ændringer i virksomhedernes fremtidige adfærd og kultur. Teknologier og digitalisering vil være nøglen til dette, og mange virksomheder er allerede i gang med at flytte flere af deres applikationer til skyen i forbindelse med e-mails, dokumentsamarbejde og lagring af filer. Disse teknologier medfører nye risici men gør det også muligt for sikkerhedsteams selv at designe sikkerheden fra bunden og bevæge sig væk fra ældre it-systemer.



Hvordan kan virksomhederne imødegå de nye cybertrusler?

Virksomhederne bør træffe tre primære foranstaltninger med henblik på at imødegå de nye cyber-risici, der opstår ved kriser som fx COVID-19:

1. Sikre ny-implementerede procedurer for hjemmearbejde.
2. Sikre kontinuitet i kritiske sikkerheds-funktioner.
3. Imødegå opportunistiske angreb, hvor der gøres forsøg på at udnytte krisesituationen.

Det anbefales også, at virksomhederne i det omfang, det er muligt, implementerer "quick-win" sikkerhedskontroller og maksimerer mulighederne for at forebygge, opdage og reagere på trusler i betragtning af øget brug af digitale systemer og værktøjer og den afledte risiko for opportunistiske angreb.

1. Sikre ny-implementerede procedurer for hjemmearbejde

Hold øje med skygge-it og flyt brugere til godkendte løsninger
Gennemgå logs over webtrafik med henblik på at holde øje med brugen af skygge-it (fx fildeling, videomøder og samarbejdsværktøjer), og arbejd på at implementere og flytte brugere til forretningsgodkendte og sikrede løsninger (fx brug af Cloud Access Security Brokers og Web Proxy Filtering).

Sørg for, at der er foretaget fuld patching og sikker konfiguration af fjernadgangssystemer
Gennemgå alle fjernadgangssystemer med henblik på at sikre, at alle kritiske sikkerheds-patches samt sikre konfigurationer er anvendt.

Identificér eventuelle sårbarheder eller forkert konfiguration ved hjælp af penetrationstests eller red teaming.

Samarbejd med it-teams om integrering af hurtige og fleksible sikkerhedstests i anvendelsen af de nye fjernadgangssystemer.

Der skal også anvendes sikker konfiguration for e-mail, identitetsstyring, (fx Active Directory) og mødesystemer, som anvendes af medarbejdere, der arbejder hjemme, fx ved at slå ældre autentificeringsprotokoller fra.

Sørg for, at sikkerhedskontroller, som findes på arbejdspladsen, stadig virker på systemerne, når medarbejderne ikke er på det interne netværk
Kortlæg de netværksbaserede sikkerheds-kontroller, som anvendes på enhederne, når medarbejderne er på det interne netværk, og evaluér, om der fortsat anvendes en lignende kontrol for netværkstrafikken fra systemer, der ikke er på det interne netværk.

Verificér, at søgninger på nettet er sikret via webfiltre, når der arbejdes hjemmefra. Hvis dette ikke er tilfældet, bør en cloudbaseret webfilterløsning anvendes med henblik på at opdage og forebygge ondsindet webtrafik.

Konfigurér dette med henblik på at begrænse de typer af websites, der kan tilgås, og de filtyper, brugerne kan downloade, og blokér adgangen til nyregistrerede eller mistænkelige domæner.

Verificér, at DLP og andre sikkerhedskon-troller på bærbare computere fungerer som forventet, når enhederne flyttes fra det interne netværk i en længere periode.

Hold øje med uregelmæssig login-aktivitet på fjernadgangssystemer, e-mail og Active Directory
Konfigurér fjernadgangsløsninger, e-mailsyste-

mer og Active Directory således, at al autentificeringsaktivitet logges.

Gem logs og analysér disse for uregelmæssig aktivitet, herunder forsøg på at bryde passwords, login fra ukendte steder og login, der indikerer "impossible travel".

Overvåg og reagér på problemer, der opstår hos medarbejdere, der arbejder hjemmefra

Overvåg it-helpdesk med henblik på at identificere klager fra medarbejdere over processer, kontroller eller teknologiske begrænsninger, der hindrer dem i at arbejde hjemmefra. Samarbejd med it-teams om at skabe fleksible løsninger, der gør det muligt for medarbejderne at være produktive, samtidig med at de forhindres i at omgå eksisterende processer.

Hjælp medarbejderne med at arbejde sikkert hjemmefra

Jeres samarbejdspartner inden for uddannelse og læring af medarbejderne eller jeres HR-afdeling bør være i stand til rulle et kort uddannelsesmodul om "hjemmearbejde" ud, som kan hjælpe medarbejderne med at forstå de potentielle trusler og sikkerhedsforanstaltninger, der kan være behov for, når de arbejder hjemmefra. Hvis ikke, så prøv at udarbejde et kort faktablad eller en kort vejledning til medarbejderne.

Det er vigtigt, at medarbejderne ved, hvor de kan hente hjælp, og at det gøres let for dem at spørge til råds og rapportere bekymringer.

Gennemgå taktiske foranstaltninger og implementér væsentlige sikkerhedskontroller, der måske er blevet overset, med tilbagevirkende kraft

Gennemgå alle bærbare computere eller servere, der er anvendt til brug for medarbejdernes hjemmearbejde, og sørg for, at de har væsentlige sikkerhedskontroller, herunder fuld diskkryptering, beskyttelse mod malware, beskyttelse mod datatab, automatiske backupløsninger samt endpoint detection og response-opsætning.

Gennemgå nye applikationer, værktøjer eller systemer etableret til brug for medarbejdernes hjemmearbejde, herunder cloudbaseret e-mail og systemer til dokumentsamarbejde (fx Microsoft OneDrive, Google Drive, Zoom, Skype) for at sikre, at væsentlige sikkerhedskontroller er anvendt ensartet.

Sørg for, at fjernadgangssystemer er tilstrækkeligt robuste over for DDoS-angreb

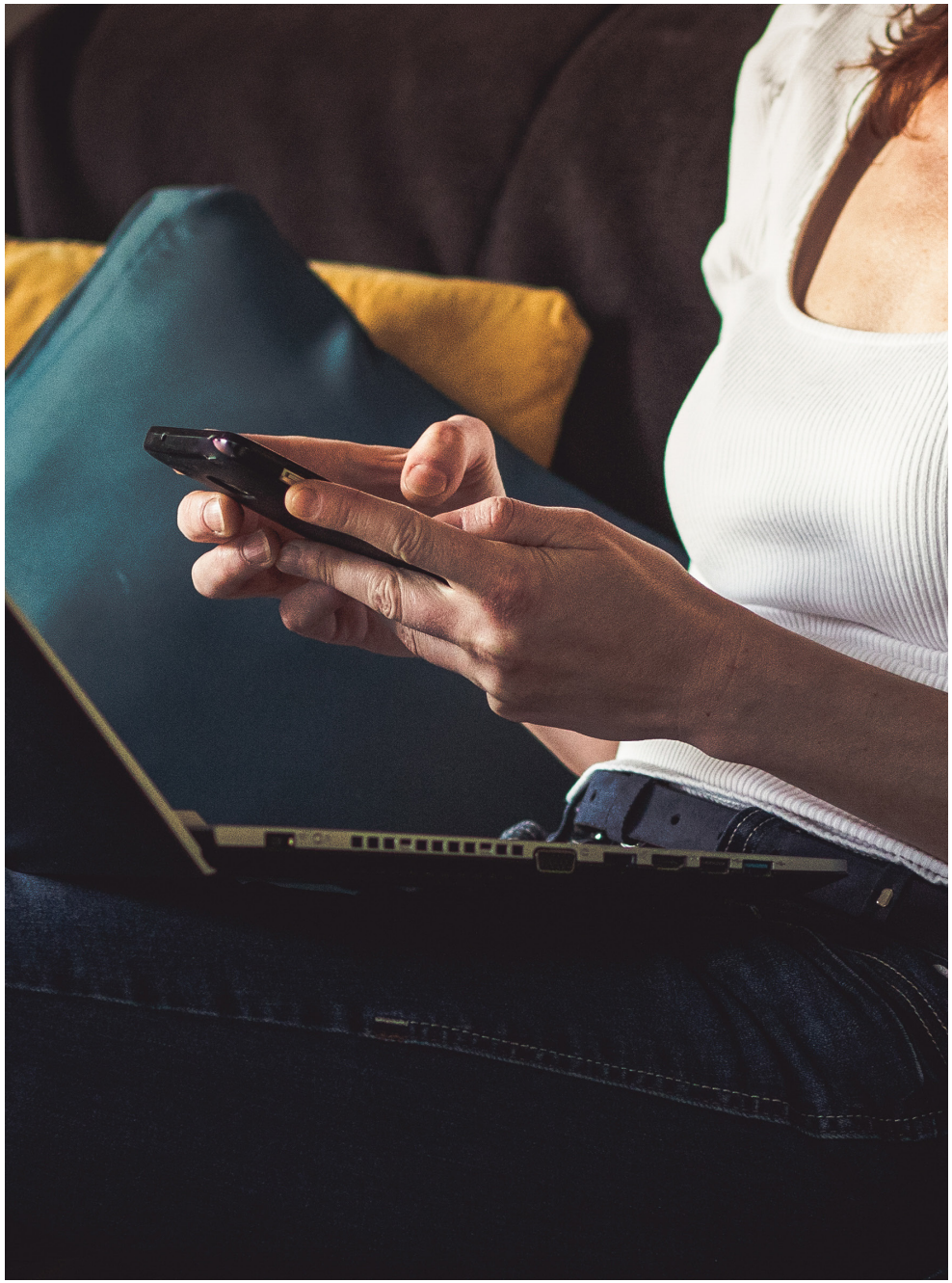
Sikkerhedsteams bør i samarbejde med it-afdelingen opnå en forståelse af fjernadgangssystemets robusthed over for DDoS-angreb, herunder en gennemgang af tilgængelig båndbredde, begrænsninger i software til fjernadgang, og hvorvidt der kan tilføjes DDoS-beskyttelse.

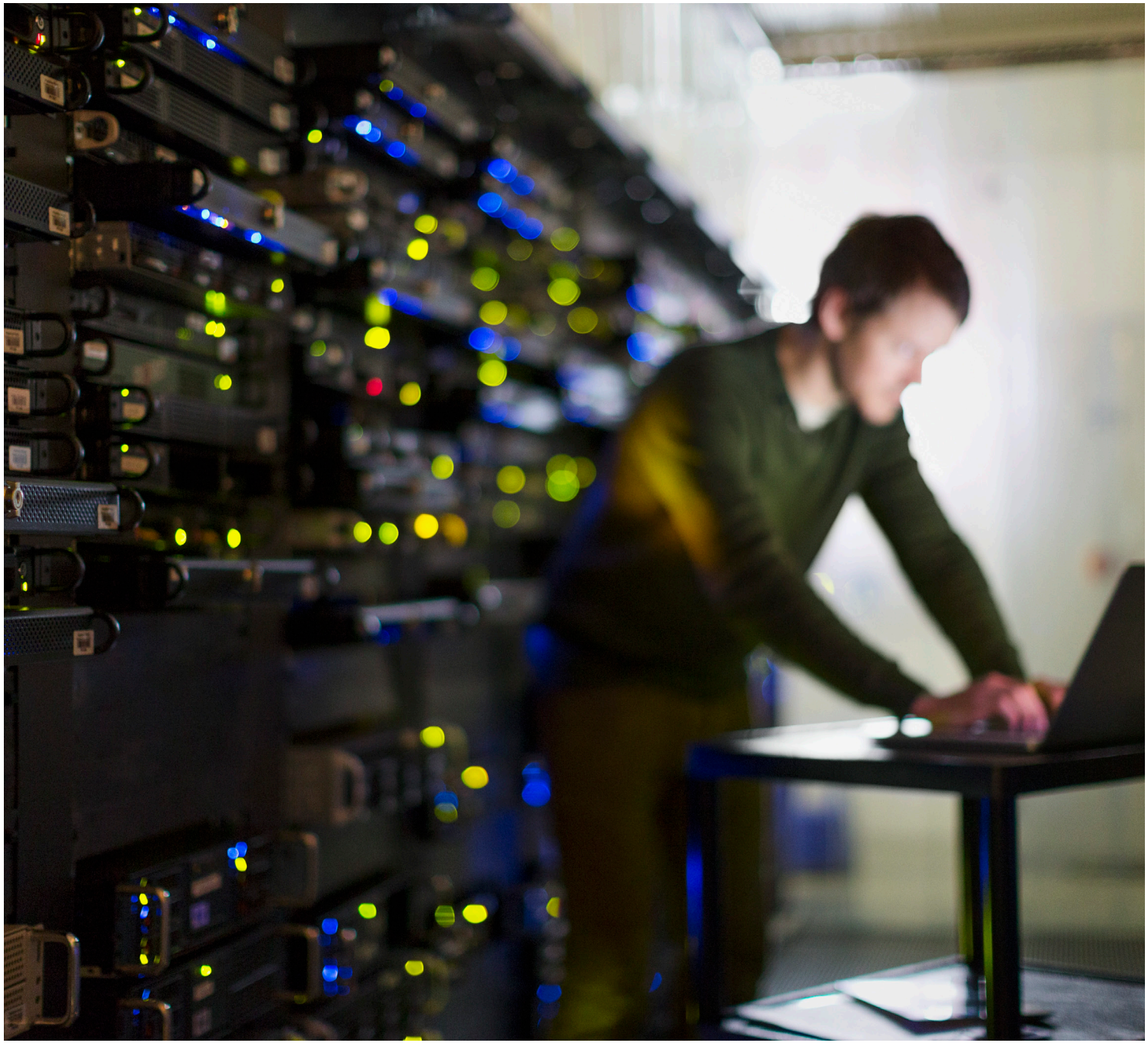
Med henblik på at sikre robusthed bør virksomhederne desuden overveje at implementere et sekundært fjernadgangssystem, som gør det muligt for administratorer at få adgang til kritiske interne systemer i tilfælde, hvor de primære fjernadgangssystemer er offline.

2. Sikre kontinuitet i kritiske sikkerhedsfunktioner

Identificér og overvåg kritiske sikkerhedsaktiviteter med henblik på at sikre kontinuitet

Identificér de aktiviteter, der er afgørende for styring af cybersikkerhedsrisikoen, fx patching





af sikkerhedssårbarheder, sikkerhedsovervågning, identitetsstyring og backup af vigtige systemer.

Sørg for, at der er identificeret tilstrækkelige ressourcer (med en margin) til at levere disse kritiske ydelser, og fastlæg, hvordan ledelsen kan overvåge udførelsen af disse aktiviteter.

Verificér, at patchingprocesser fungerer, herunder for bærbare computere, der benyttes til hjemmearbejde

Verificér, at patchingprocesser fortsat virker, når systemerne ikke er på de interne netværk, og test, at de anvendte patches eller opdateringer ikke påvirker medarbejdere, der arbejder hjemmefra.

Sørg for, at de etablerede planer for out-of-band patching fortsat er gældende, og overvej, hvordan fjernadgangssystemerne skal patches, da de nu er kritiske for forretningsdriften.

Foretag løbende intern vurdering af sårbarhedsniveauet for at verificere, at patchingprocesserne fungerer, og at alle kritiske sårbarheder er patchet eller afhjulpet.

Sørg for at sikre internetvendte applikationer og ydelser

Gennemfør løbende interne og eksterne vurderinger af sårbarhedsniveauet med henblik på at identificere kritiske sårbarheder i internetvendte systemer, og at eksponerede systemer og tjenester, der er nødvendige, er særligt sikret.

Overvej at bruge cloudbaserede løsninger for at opnå hurtig udnyttelse og skalerbarhed med konfigurering af løbende scanning af interne og eksterne tjenester og webapplikationer

samt advarsel om nye eksterne sårbarheder og eksponerede tjenester.

Indfør stop for it-ændringer på systemer med høj risiko, hvis de normale processer ikke kan følges grundet mangel på medarbejdere

Konfigurationsændringer til systemer med høj risiko eller systemer, som ofte kan blive konfigureret forkert (fx firewall-adgang omkring cloudhostede databaser) bør begrænses. Alternativt bør der etableres yderligere godkendelsesprocedurer med henblik på at sikre, at der ikke foretages ændringer uden tilstrækkelige overvejelser eller ved en fejltagelse.

Gennemgå, hvorledes privilegerede brugere anvendes

Sikring og adskillelse af privilegeret adgang er afgørende for at kunne forhindre it-kriminelle i at kompromittere kritiske brugerprofiler og det bredere netværk.

Mange virksomheder bruger dedikerede administrator-terminaler eller 'privileged access management-løsninger' til at opnå dette og bør sikre sig, at disse kan fortsætte med fjernadgang (fx ved at stille yderligere bærbare computere med strengere sikkerhedskontroller til rådighed).

Virksomhederne bør ligeledes sikre, at der fortsat opretholdes gode sikkerhedsprocedurer vedrørende administration på trods af presset for at foretage hurtige ændringer i it-miljøet.

Det bør desuden overvejes, hvorvidt det er nødvendigt at etablere backupmetoder til sikker administration. Hvis systemerne fx begrænser administratoradgang baseret på IP-range, kan denne adgang blive afbrudt, hvis fjernsystemerne går ned.

Sørg for, at virksomheden har de nødvendige medarbejdere, processer og den teknologiske kapacitet til at opdage og reagere på cyberangreb

Sørg for, at virksomhedens teams har de medarbejderressourcer og adgang til de processer og den teknologi, der er nødvendig for at overvåge og reagere på advarsler (med en hensigtsmæssig margin). Overvej at tilføre Security Operations teams yderligere ressourcer eller benytte en managed service under anvendelse af Endpoint Detection og Response-teknologi.

Overvej desuden integration med automatiserings- og orkestreringsværktøjer, som kan bidrage til at reducere personafhængigheden og sikre kontinuitet på trods af medarbejderreduktion.

Opdatér incident response-planer og håndbøger for at sikre, at de fungerer med en arbejdsstyrke, der primært arbejder hjemmefra

Gennemgå incident response-processer (herunder frameworks, håndbøger og runbooks) for at sikre, at de er opdaterede og fungerer med en arbejdsstyrke, der arbejder hjemmefra.

Opnå forståelse af, hvordan der opnås adgang til endpoint telemetry og data med fjernadgang med henblik på undersøgende arbejde, og test, at de ansvarlige medarbejdere har den nødvendige adgang og uddannelse.

Sørg også for, at processerne ikke er alt for afhængige af nøglemedarbejdere, og beskriv klart, hvilke foranstaltninger der skal træffes i tilfælde af hændelser, så mindre erfarne medarbejdere kan implementere dem.

Forbered jer på, at et cyberangreb og sikkerhedsbrud kan være et brud på persondatasikkerheden. Vi anbefaler at have ressourcer



Sørg for, at virksomheden har de nødvendige medarbejdere, processer og den teknologiske kapacitet til at opdage og reagere på cyberangreb.

med i incident processen, som har kendskab til gældende lovgivning fx GDPR, og som kan bistå med vurdering af, om der er tale om et brud på persondatasikkerheden. I den sammenhæng kan det være en god ide, at have en tjekliste klar med typer af sikkerhedshændelser og en indledende risikovurdering, herunder vudering af, om sikkerhedsbruddet skal anmeldes til Datatilsynet, og om de registrerede skal underrettes.

Anvend asset management-værktøjer til at sikre fortsat synlighed, efterhånden som systemerne flyttes væk fra det interne netværk

Asset management-værktøjer gør aktiverne synlige, uanset hvor de befinder sig, og viser, om de er i overensstemmelse med sikkerhedskontrollerne (fx om systemerne er patchet og kører på en opdateret remote access client-version), hvilket er af afgørende betydning. Asset management-værktøjer er nøglen til at sikre, at sikkerhedsværktøjerne anvendes i fuldt omfang på alle systemer.

3. Imødegå opportunistiske angreb, hvor krisesituationen udnyttes

Fokusér på at skabe yderligere opmærksomhed og kommunikation, når der opstår nye trusler

Den support, der gives til medarbejderne, så de kan arbejde sikkert hjemmefra, bør på det rigtige tidspunkt styrkes med målrettet kommunikation om relevante nye trusler. Dette omfatter på nuværende tidspunkt målrettede anti-phishing-kampagner, samt at fremhæve over for økonomifunktionen, at der er øget risiko for angreb, hvor virksomhedens e-mailkonti kompromitteres i forsøg på at udnytte, at der anvendes anderledes eller nye arbejdsmetoder.

Phishingangreb er i år den hyppigst oplevede angrebstype. Hele 79 % af de virksomheder, der har oplevet et cyberangreb, vurderer, at deres virksomhed har været udsat for et phishingangreb. Det er en stigning på hele 11 %-point i forhold til sidste år, og dermed ligger antallet på det hidtil højeste niveau. Det viser PwC's Cybercrime Survey 2020.

Kommunikationen skal være understøttende og nyttig og bør gennemgås af kommunikationsmedarbejdere, så det sikres, at den udsendes på det rigtige tidspunkt og i et sprog, der ikke giver anledning til yderligere bekymring eller forvirring.

Sørg for at have én enkelt "kommunikationskilde" i virksomheden, hvad angår tiltag og ændringer som følge af COVID-19 for at begrænse sandsynligheden for, at medarbejderne lokkes til at klikke på potentielt ondsindede beskeder.

Vejled specifikt medarbejderne i at være ekstra på vagt over for anmodninger om personlige eller økonomiske oplysninger eller anmodninger om pengeoverførsler

Medarbejderne bør vejledes specifikt med henblik på at sikre, at de ikke svarer på e-mails, hvor der bedes om personlige eller økonomiske oplysninger, eller anmodes om pengeoverførsler.

Økonomifunktionen bør gennemgå betalingsprocedurerne for at sikre, at de fortsat er robuste i nye arbejdsmiljøer, og økonomimedarbejderne bør have bemyndigelse til at udvise omhu i forbindelse med godkendelse af usædvanlige betalingsanmodninger fra ledende medarbejdere, fx ved at kontakte dem for at indhente bekræftelse via en separat sikker kommunikationskanal.

Imødegå den øgede risiko for insidertrusler i tilfælde af afskedigelser eller opsigelser

Udarbejd planer for hurtigt at begrænse opsagte medarbejderes adgang til systemer og data med henblik på at reducere risikoen for, at der stjæles data eller forvoldes skade på systemer.

Da virksomhederne muligvis ikke vil kunne indhente enheder fysisk fra medarbejderne, skal planerne have fokus på at deaktivere adgang til fysiske enheder, konti og systemer på netværket.

Overvej at implementere yderligere logning for medarbejdere, som kan udgøre en risiko, med gennemgang af de handlinger, der udføres af disse medarbejdere, og anvendelse af målrettede DLP-politikker for at forhindre eksfiltration af data.

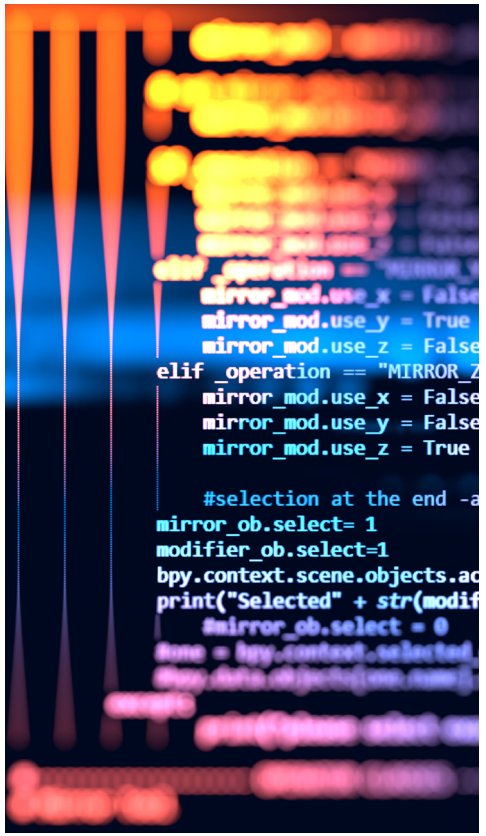
Imødegå den øgede risiko for phishing med tekniske kontroller

I betragtning af den øgede risiko for cyberangreb i en krisetid bør det overvejes at implementere yderligere tekniske kontroller med henblik på at reducere truslen fra phishing-mails. Dette bør omfatte opsætning af avancerede filtreringsløsninger med henblik på at identificere mistænkelige e-mails, samt konfigurering af filtreringsteknologi for at hvidliste de filtyper, brugere kan modtage som vedhæftninger til e-mails eller downloade fra internettet.

Anvend tekniske kontroller, der giver "quick-wins", i hele it-miljøet, hvor det er muligt

I betragtning af den øgede kortsigtede afhængighed af teknologien og risikoen for nye opportunistiske angreb bør virksomhederne desuden søge at anvende tekniske kontroller, der giver "quick-wins", med henblik på at reducere risikoen.

Væsentlige risici, som disse kontroller bør rettes imod, er phishing-mails, angreb ved at sprede ondsindede koder på arbejdsstationer og servere samt lateral movement-aktiviteter.



Kontakt

Likviditetsstyring i en krisetid



René Brandt Jensen
Partner
M: 2141 6025
E: rene.brandt.jensen
@pwc.com



Mads Johansson
Partner
M: 2321 1412
E: mads.johansson
@pwc.com

Fem trin til at få styr på omkostningerne



Natasha Lembke
Partner
M: 5133 1677
E: natasha.lembke
@pwc.com



Søren Blok Jensen
Partner
M: 3053 6625
E: soren.blok.jensen
@pwc.com



Jim Christian Olesen
Director
M: 5150 7198
E: jim.christian.olesen
@pwc.com

Skab en robust supply chain



Bo Dencker
Partner
M: 4075 3999
E: bo.dencker
@pwc.com



Jens Arvad Johansen
Director
M: 4042 4550
E: jens.johansen
@pwc.com

Kontakt

Risikostyring i en krisetid



Brian Christiansen
Partner
M: 5140 8040
E: brian.christiansen
@pwc.com



Jeanne Koch Rasmussen
Director
M: 2961 2462
E: jeanne.koch.rasmussen
@pwc.com

Forbered din organisation til fremtiden



Kim Domdal
Partner
M: 3070 1853
E: kim.domdal
@pwc.com



Anna C. von Kauffmann
Manager
M: 3068 7719
E: anna.c.von.kauffmann
@pwc.com

Cyber Security-udfordringer i krisetider



Mads Nørgaard Madsen
Partner
M: 2811 1592
E: mads.norgaard.madsen
@pwc.com



Jørgen Sørensen
Partner
M: 2494 5254
E: jorgen.jgs.sorensen
@pwc.com



pwc

Revision. Skat. Rådgivning.

Succes skaber vi sammen ...