## Cybersikkerhet – del I:

# Cybersikkerhet som strategisk pilar

**Cybersikkerhet har tradisjonelt blitt vurdert som en taktisk utfordring, ikke et strategisk fokusområde. Slik trenger det ikke å være. Stadig flere topplederе innser nå at manglende cybersikkerhet kan utgjøre en formidabel risiko for hele selskapet, dets omdømme, lønnsomhet og virke.**

Artikkelen er forfattet av:

Ph.D.
**Arne Helme**
Partner og leder for Cybersikkerhet i KPMG

I vår årlige internasjonale topplederundersøkelse anses ny teknologi som en av de fem viktigste risikofaktorene i virksomhetens hverdag. Hele 72 prosent av de spurte lederne medgir at deres virksomhet ikke er fullt ut forberedt på å takle konsekvensene av en større cyber-hendelse. Flere ser for seg å gjøre betydelige teknologi-relaterte investeringer de neste tre årene, blant annet innen cybersikkerhet. Funnene fra fjorårets undersøkelse viste det samme. Da svarte én av tre toppledere at cybersikkerhet var blant de største utfordringene for selskapet. En av fem oppga at informasjonssikkerhet var det som bekymret dem aller mest.

Cybertrussel er ikke et nytt fenomen. Oppmerksomheten rundt cybersikkerhet har likevel blitt forsterket grunnet de mange høyprofilerte, skadelige og forstyrrende hendelsene vi kan lese om i media. Vi hører om alt fra lekkasjer og tyveri av informasjon, omfattende lovbrudd og tap av data, til utro tjenere til svikt i rutiner og infrastruktur. Det er mye som står på spill, og virksomhetene må ta stilling til hvordan de vil respondere på denne økte trusselen.

### Ta den viktige helsesjekken

Med dette bakteppet er vårt råd at norske virksomheter bør øke bevisstheten når det gjelder å sikre egne verdier. I dette ligger det å ta stilling til sin egen modenhet på cybersikkerhet og løfte beredskap og planer opp på et nytt nivå.

For mange er cybersikkerhet et ukjent område. I et forsøk på klargjøring, la oss gå inn på hvilke spørsmål det er nødvendig at virksomheter stiller seg.

*Styring og ledelse*
Er eierskapet til risikostyring og cybersikkerhet forankret på toppen? Det bør inkorporeres som en sentral del av forretningsstrategien, med føringer og involvering fra toppledelsen og styret.

*Menneskelige faktorer*
En god sikkerhetskultur er alfa og omega. Hvilke holdninger har medarbeiderne? Hvilken fagkompetanse og opplæring er tilgjengelig? IT-sikkerhet handler ikke kun om bokser og ledninger. Menneskene og prosessene kommer først.

*Håndtering av informasjonsrisiko*
Det er vesentlig å kartlegge truslene virksomhetene står overfor. Hvilke planer for risikohåndtering finnes? Hvilken type forretningskritisk informasjon og intellektuelle verdier forvaltes i dag?

*Kontinuitet i forretningen*
Er virksomheten forberedt på en eventuell hendelse? Og skulle den inntreffe, har dere god krisehåndtering og dialog med ulike

interessenter, slik at dere kan minimere konsekvensene?

*Etterlevelse av lover og regler*
Innhenting og oppbevaring av informasjon er lovlig regulert. Hva gjør dere i virksomheten for å etterleve lovpålagte krav og standarder når det kommer til blant annet lagring, bruk og offentliggjøring av informasjon, håndtering av sensitive informasjon, forsikring knyttet til cyberrisiko og lignende?

Vi mener at cybersikkerhet bør dreie seg om hva du kan gjøre – ikke hva som er vanskelig å få til. Evner man å gjøre et målrettet stykke arbeid med sikkerhet, vil ikke cybertrusselen fremstå som et «ømt punkt» i virksomheten, men heller utvikle seg til en unik strategisk fordel.