

1. Strategi for risikostyring og interessentanalyse

www.cyber-smv.dk



Strategi
Strategy

Formål, deltagere og anvendelse

- **Formål**

- At få udarbejdet en strategi for risikostyring.
- At skabe et overblik over de interne og eksterne interessenter, som enten er en del af virksomheden, eller som virksomheden er afhængig af.
- At sikre opbakning til cybersikkerhedsstrategien eller bliver informeret på et passende niveau.
- At sikre en effektiv implementering af virksomhedens cybersikkerhedsstrategi.

- **Deltagere**

- Udføres af personer med indgående kendskab til virksomhedens interne og eksterne partnere, kunder, leverandører m.v.

- **Anvendelse**

- Bør udføres med en passende frekvens.

Strategi for risikostyring: Eksempler på indhold

1. Formål og scope.
2. Governance og roller.
3. Risikopolitik og appetit.
4. Risikostyringsproces.
5. Værktøjer og metoder.
6. Kommunikation.
7. Kontinuitetsplanlægning.
8. Måling og forbedring.

Opgaver efter strategiudviklingen

- **Identifikation af interessenter**
 - Kortlæg de interne og eksterne interessenter, som har betydning for strategiens succes.
- **Identificér interessenternes interesser**
 - Forstå, hvad hver interessentgruppe ønsker at opnå eller beskytte i relation til cybersikkerhed.
- **Identificér interessenternes bekymringer**
 - Afdæk eventuelle forbehold, risici eller modstand, som interessenterne måtte have.
- **Udarbejd en plan for, hvordan hver interessentgruppes interesser og bekymringer skal håndteres for at opnå opbakning til strategien**
 - Beslut, hvordan du bedst kommunikerer, involverer og engagerer de forskellige grupper for at sikre deres støtte.

Mulige interessenter, interesser og bekymringer

Interessenter	Interesser	Bekymringer
Ledelse (C-niveau) og Bestyrelse	Strategisk overblik, risikostyring, omdømme, overholdelse af lovgivning, investeringsbeslutninger	Omkostninger, ROI, kompleksitet, forretningsforstyrrelser
Indkøb	Leverandør relationer, kontrakt håndtering	Leverandør modstand, kompleksitet
IT / Cybersikkerhedsteams	Effektiv implementering, teknisk sikkerhed, systemstabilitet, trussels mitigering, hændelses respons	Resource begrænsninger, manglende opbakning fra ledelsen
Jura & Compliance	Regulatorisk risiko, kontraktvilkår	Ansvar, revisionsrettigheder
Leverandører	Forretningskontinuitet, Lethed ved at drive forretning, kontrakt overholdelse	Omkostninger ved overholdelse
Operations / Logistik	Kontinuitet i forsyningen, modstandsdygtighed	Risiko for forstyrrelser
Kunder / Klienter	Beskyttelse af persondata, tillid, servicekontinuitet,	Databrud, manglende gennemsigtighed, dårlig håndtering, data beskyttelse
Investorer / Aktionærer	Risikoeksponering	Værdipåvirkning
Forsikringsvirksomheder	Præcis (cyber) risikovurdering, politikoverholdelse	Præmieberegning

Andre interessenter, interesser og bekymringer

Interessenter	Interesser	Bekymringer
Tilsynsorganer & offentlige myndigheder	National sikkerhed, regelhåndhævelse, økonomisk stabilitet	Offentlig sikkerhed
Standardiserings organisationer & Industriorganisationer	Best practices, harmonisering	Sektor-bred modstandsdygtighed
Samfund / Generel offentlighed	Databeskyttelse, kontinuitet af kritisk service tilgængelighed (mad, vand, osv.)	Offentlig rapportering omkring cybersikkerhed og modenhed, transparent dokumentation
Medie og vagthunde organisationer	Offentlig ansvarlighed	Transparens i håndteringen af hændelser
Cybersikkerhedsforums & Informationsdelingsgrupper	Trussel efterretningsdeling	Kordinerede respons

Listen er ikke udtømmende, men er tænkt inspiration

Potentielle steps for interessentstøtte

1. Udarbejd en klar business case

- Kvantificér risici (f.eks. omkostninger ved brud i forsyningskæden, nedetid, tab af kunder).
- Fremhæv regulatoriske og kommercielle konsekvenser (f.eks. NIS2, GDPR).
- Understreg konkurrencefordele: tillid, robusthed, adgang til kontrakter.

2. Tilpas budskabet

- Direktionen: Fremhæv finansielle og omdømmemæssige risici, juridisk ansvar og sammenhæng med ESG/CSR.
- Indkøb: Fokuser på effektivitet, leverandørvurdering og forenkling af kontrakter.
- IT: Vis hvordan strategien integreres med eksisterende kontroller og arkitektur.
- Leverandører: Tilbyd støtte og modeller for trinvis overholdelse for at lette implementeringen.
- Osv.

3. Interessentworkshops og samskabelse

- Afhold workshops for at indsamle input fra alle (relevante) interessenter.
- Afprøv strategien på en mindre gruppe leverandører for at teste gennemførlighed og foretage justeringer.