# Cyber Risk Mapping

Cyberrisker förändras ständigt, är svåra att förutsäga och oftast väldigt komplicerade. Skadorna kan också bli förödande och ta lång tid att lösa. I 2017 års Global Risk Management Survey klättrade cyber upp till plats nummer fem som företagens största risker. Varje företag som har en webbplats, använder mobil teknik och smartphones har en riskexponering för olika typer av cyberbrott.

Att kartlägga ett företags riskexponering är ett första steg till att förstå det skyddsbehov företaget har. Aons riskingenjörer har vidareutvecklat en metod för att identifiera, kartlägga och utvärdera nuvarande strategier för risk management samt klassificera riskexponeringen för de cyberrisker som finns inom ett företags verksamhet. En sådan kartläggning kan också utgöra ett beslutsunderlag för eventuellt behov av en cyberförsäkring.

## Visualisera och värdera

Risk mapping är en arbetsprocess som innebär att risker och riskexponeringar visualiseras i en matris och värderas utefter två variabler. Hur stor påverkan skulle en identifierad risk ha på verksamheten och hur väl förberedd är företaget att hantera den risken? Termen riskfaktor används för att beskriva hur väl en risk hanteras inom företaget.

## Vem kan verksamheten bäst?

Resultatet av en risk mapping är helt beroende av de personer från företaget som deltar i workshopen. Det är den egna personalen som bäst känner till verksamheten. Aon kompletterar med specialistkompetens inom cyberrisk och cyberförsäkring men övningen bygger på att företaget själva lyfter och diskuterar de risker som de ser som kritiska för sin verksamhet. Det förutsätter också att närvarande personer har god insikt i företaget verksamhet, dess IT-lösningar samt de funktioner som är beroende av datamiljön.

## Hur går det till?

En risk mapping är generellt en heldags-aktivitet med utvalda nyckelpersoner från företagets olika verksamhetsområden. Grunden styrs av företagets unika förutsättningar men processen är liknande för alla företag som genomför en cyber risk mapping.  Det är deltagarna själva som i huvudsak är aktiva i diskussionerna och Aons riskingenjör fungerar som stöd och moderator. Detta för att säkerställa att diskussionerna är relevanta för övningen och leder fram till ett konkret och användbart resultat.

## Workshopens fyra delar:

**Del 1 - Introduktion:** Våra erfarna riskingenjörer identifierar de huvudsakliga IT-risker som företaget exponeras för. Identifieringsprocessen bygger på intern kunskap, därför rekommenderar vi att deltagare från flera delar av företagets verksamhet deltar.

**Del 2 - Brainstorming:** Rundabordsdiskussioner om vilka konsekvenserna är för de identifierade riskerna vid ett eventuellt systemhaveri. Varje risk kategoriseras som låg, medium, hög eller extrem påverkan på företaget. Gemensamma kriterier omfattar: avbrottstider, finansiella kostnader, marknadseffekter, leveransmöjligheter till kund samt effekter på respektive avdelning.

**Del 3 - Konsekvens:** I detta steg definieras den nuvarande nivån av hantering för de identifierade riskerna. Detta inkluderar faktorer såsom överensstämmelse mellan lokala och regionala lagar och förordningar, tillfredsställande tekniska säkerhetssystem, utbildning för personal samt resurser.

**Del 4 - Riskbild:** Riskerna placeras i en matris som visar de mest kritiska risker som identifierats. Aons specialistmäklare kommer därefter att ge rekommendationer om vilka risker och situationer som är försäkringsbara och hur man som företag bör gå vidare.

## Kontakta oss

För mer information om cyber risk mapping kontakta:


Julian Ademius
julian.ademius@aon.se
T: 072 080 24 52

Daniel Holm
daniel.holm@aon.se
T: 070 495 84 95

Matti Seiman
matti.seiman@aon.se
T: 073 022 77 67


Empower Results®

## Reslutatet

Resultatet av en risk mapping är dels en analytisk rapport där alla risker och workshopens olika diskussioner sammanfattas samt riskmatrisen som levereras som editerbart dokument för att företaget själv ska kunna flytta eller lägga till/ta bort risker vartefter förändringar sker. Företaget får också rekommendationer från Aons riskingenjörer om hur de bör/kan gå vidare baserat på resultatet.

En risk mapping utgör ett bra underlag för hur identifierade risker ska hanteras/ bearbetas. Lösningen kan vara att förbättra det interna skyddet eller säkerställa att det finns försäkringstäckning. En risk mapping ger också en fingervisning av vad de finansiella konsekvenserna av exponeringen kan bli och utgöra en grund för att diskutera limiter för en cyberförsäkring.

## Cyberförsäkring

På vår hemsida finns mer information om våra olika lösningar för att hantera cyberrisker och andra försäkringsformer. Besök oss på: www.aon.se för att läsa mer om våra produkter och tjänster.

## Förslag på deltagare

- Insurance Manager
- CFO
- IT Manager
- Area Managers (IT/ IS)
- IT Developer
- IT System Owner
- E-commerce Manager
- Customer Service
- Operation Manager
- Logistic Manager
- Warehouse Manager
- Supplier Manager
- Legal