Cyber Risks

Tirsdag den 5. december 2017 kl. 17.00 – 19.00 med efterfølgende reception
Kromann Reumert, Sundkrogsgade 5, 2100 København Ø

Det er blevet afgørende for virksomheder at identificere, følge og evaluere kendte såvel som endnu ukendte Cyber relaterede risici – og at etablere relevante forsvarsmekanismer og "Contingency Plans".

Cyber Risks og Cyber Risk Management er i dag højt prioriteret på dagsordenen i den øverste ledelse, i selskaberne, hos offentlige myndigheder og på nationalt plan. I det kommende forsvarsforlig lægges der op til at styrke Center for Cybersikkerhed, bl.a. ved at etablere et center for tidskritisk udveksling af information om trusler og angreb. I den finansielle sektor, hvor 80 procent af transaktionerne i dag er digitale, har Nationalbanken etableret Finansielt Sektorforum for Operationel Robusthed (FSOR). Meget store finansielle virksomheder, som fx Barclays Bank, indgår i transnationale samarbejder om at identificere, modvirke og bekæmpe Cyberangreb og kriminalitet.

Flere end hver tredje virksomhed er allerede udsat for Cyberangreb, og alle virksomheder er i fare for at blive angrebet, lyder vurderingen fra erfarne topledere. Det er indtil nu mest de store virksomheder, som man hører om. Mærsk anslår, at skaderne efter sommerens NotPetya angreb kan løbe op i 2 mia. kr. I maj og juni 2017 blev 143 millioner amerikanske forbrugere udsat for, at personlige oplysninger blev hacket hos kredit rating bureauet Equifax. Ved samme lejlighed stjal hackerne 209.000 kreditkort numre. Uber har forsøgt at betale hackerne for at holde historien ude af offentligheden - det holdt et år. De årlige investeringer i Cyberforsvar anslås at have passeret 1.000 mia. kroner. Efterspørgsel efter Cyberkompetencer vokser 3 gange hurtigere end til andre IT relaterede jobs.

Hvilke trusler er det tale om? Hvem står bag? Hvad kan forventes fremover? Hvad er bestyrelsens opgave, og hvordan kan det gribes bedst an? Hvilken rolle har Center for Cybersikkerhed, og hvordan kan virksomhederne drage nytte heraf? Hvilke virksomheder kan med fordel også deltage i transnationalt samarbejde? Hvad gør man, når angrebet er der? Hvordan ser en best practice contingency plan ud?

Disse og relaterede spørgsmål belyses ved konferencen den 5. december med deltagelse af Group Chief Security Officer Troels Ørting, Barclays Bank; Director Thomas Lund-Sørensen, Center for Cybersikkerhed, Forsvarets Efterretningstjeneste; Chief Financial, Strategy & Transformation Officer Jakob Stausholm, Transport & Logistics division, Maersk. I paneldebatten medvirker bestyrelsesformand Sanna Suvanto-Harsaae og partner Torben Waage, Kromann Reumert.

Agenda

17.00	**Velkomst og introduktion** *Tom Jacobsgaard*
17.05	**Cyber Risks - Hvilke trusler er det tale om? Hvem står bag? Hvad kan forventes fremover? Hvad er bestyrelsens opgave, og hvordan kan det gribes bedst an?** *Troels Ørting*
17.45	**Cyber Risks - Hvilke trusler er det tale om? Hvem står bag? Hvad kan forventes fremover? Hvilken rolle har Center for Cybersikkerhed, og hvordan kan virksomhederne drage nytte heraf?** *Thomas Lund-Sørensen*
18.10	**Angrebet på Mærsk i sommeren 2017 - Hvad gør man, når angrebet er der? Hvilke er væsentlige læringspunkter? Overvejelser om governance og risk management fremadrettet.** *Jakob Stausholm*
18.40	**Paneldebat om best practice fremadrettet, i virksomhederne og på nationalt plan** *Sanna Suvanto-Harsaae, Troels Ørting, Thomas Lund-Sørensen, Jakob Stausholm* *Facilitatorer: Torben Waage og Tom Jacobsgaard*
19.00	**Afrunding og let reception**