Data og internetsikkerhed bør inddrages i ledelsens fokusområder

Af Klaus Stubkjær Andersen, partner, og Tine Olsen, juridisk konsulent, WIllis

Inden for det seneste årti er fokus på ledelsesansvar steget markant, hvilket sandsynligvis kan tilskrives både de mange ledelsesansvarssager, hvoraf kun et fåtal har været nævnt i medierne, og den stigende fokus på "Corporate governance" (god selskabsledelse).

God selskabsledelse kræver overblik, gennemsigtighed og ansvar. Dette betyder bl.a., at ledelsen kontinuerligt bør undersøge og monitorere hvilke risici virksomheden står overfor, hvilke der kan minimeres og hvilke risici virksomheden kan afdække ved at tegne forsikring.

Cyber risici

Bortkomst eller tyveri af data og hacking truer i stigende grad danske virksomheder, og flere danske virksomheder har allerede stiftet bekendtskab med fjendtlige angreb på deres systemer/netværk.

En ny undersøgelse viser, at mere end 85% af 258 risk managers, it-ansvarlige, bestyrelsesmedlemmer m.fl. indikerer, at virksomheds største risici pt. er cyber. Dette overgår andre områder, såsom tab af indtægt, skade på løsøre og investeringsrisici. Tillige indikerede 80% at de finder det vanskeligt, at følge med, fordi truslen fra cyberspace udvikler sig i så højt et tempo.

Truslen fra "cyberspace" er aktuel og reel, idet alle virksomheder i dag er afhængige af interne og eksterne systemer, hvor data i stigende omfang transporteres via et netværk eller internettet. Og virksomheders netværk, systemer og ikke mindst data – uanset om det er virksomhedens egne data eller data der opbevares for andre – er blevet et attraktivt mål for hackere i hele verden.
Virksomhedens ledelse og risk managers bør derfor ikke undervurdere de risici, der følger med, når man bevæger sig i en verden bestående af moderne teknologi.

Ledelsens fokus på risikostyring og forsikring i forhold til data- og internet sikkerhed

I en ny rapport fra the World Economic Forum opfordres ledelsen(bestyrelsen og direktionen) til at tage ansvar for virksomhedens data- og internetsikkerhed. Ledelsen bør være involveret i en kontinuerlig beslutningsproces vedrørende virksomhedens it-sikkerhedspolitik og bør ikke overlade ansvaret herfor til virksomhedens risk manager eller it-chef, for der er ikke alene tale om en praktisk eller teknologisk udfordring.

"If you think technology is the solution to your cyber security risk, you neither understand technology or your cyber security risk."

For at kunne lede virksomheden og medarbejderne bedst muligt, skal ledelsen have indsigt i – og udstede klare instruktioner om virksomhedens – it-sikkerhedspolitik, herunder dataopbevaring og sikkerhedsopdatering. Desuden skal ledelsen i samarbejde med den it-ansvarlige udarbejde en it-beredskabsplan, som kan begrænse omfanget af skaden (f.eks. hacking eller lækage af data) når den sker.

En it-sikkerhedspolitik og en it-beredskabsplan hjælper virksomheden og ledelsen et skridt på vejen i kampen mod hacking, men hvis uheldet er ude eller man bliver mål for en eller flere hackeres kriminelle handlinger, så er der praktisk talt næsten intet, der kan stoppe dem.
Derfor bør alle virksomheder overveje at tegne en Data- og Netforsikring, som kan afdække en del af de risici, der er forbundet med et angreb i "cyberspace" og/eller ved opbevaring af data.

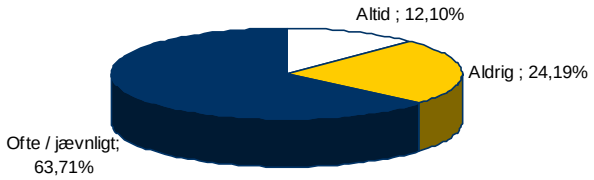
Hvad gør bestyrelsen for at minimere risici i forhold til data- og internet sikkerhed?

Når man taler om it-kriminalitet og tyveri af følsomme/hemmelige oplysninger er et andet centralt emne bestyrelsens håndtering af fortroligt materiale.

"Board Governance 2012" undersøgelsen, foretaget af Thomson Reuters viser, at over 70 % af de adspurgte bestyrelser anvender private computere, tablets og mail-konti m.m. til bestyrelsesarbejdet. Disse er ofte usikre og anvendes til andre formål end bestyrelsesarbejdet. Dette øger risikoen for, at fortroligt data lækkes, idet det er "nemt" for en hacker, at skaffe sig adgang hertil, f.eks. via online mailkonti. I flere tilfælde har be-

styrelser desuden oplevet, at et bestyrelsesmedlem enten er blevet bestjålet eller har forlagt fortrolige dokumenter (eller pc-udstyr indeholdende fortrolige dokumenter).

Bestyrelsen sender dokumenter til bestyrelsesmedlemmer ved at anvende private, online emails, såsom Hotmail, Gmail m.v.



Willis anbefaler, at bestyrelsen overvejer hvordan fortroligt data fremsendes til de enkelte bestyrelsesmedlemmer, hvordan det opbevares og hvordan det destrueres.
Der findes løsninger på det danske marked, som er specielt designet til sikker og nem deling af forretningskritiske dokumenter og processer, herunder særligt bestyrelsesarbejdet.

Hvad kan ledelsen gøre for at begrænse virksomhedens og egne personlige risici?

Konsekvenserne af it-relaterede risici kan forhindres eller minimeres ved forebyggende foranstaltninger og klare retningslinjer.

Ledelsen kan gøre meget og i ventureselskaber og kapitalfonde kan følgende spørgsmål danne grundlag for en diskussion af risici og hvordan disse håndteres:

1. Har virksomheden/fonden udarbejdet en it-sikkerhedspolitik?
2. Hvilke data kan blive kompromitteret, såfremt jeres netværk hackes?
3. Hvilken risiko vil det udgøre for selskabet/fonden, såfremt netværket/systemet hackes og hackerne opnår adgang til opbevaret data?
4. Vil det være muligt for en hacker, at ændre eksisterende data eller ”plante” falsk data i jeres system, om kan påvirke en investering?
5. Vil det påvirke selskabets/fondens renommé, såfremt offentligheden får kendskab til at data er lækket?
6. Hvilket tab vil selskabet/fonden lide, såfremt jeres systemer/netværk bryder ned pga. hacking eller virus?
7. Har virksomheden/fonden kontinuerlig backup af data?
8. Hvilken it-sikkerhed skal forhindre et hacking angreb eller datalækage?
9. Har selskabet/fonden budgetteret med udgifter til genetablering af data, notifikation af de involverede, PR, udredning af angrebet, herunder udgifter til it-konsulenter og advokatbistand?
10. Er ovenstående risici afdækket på jeres nuværende forsikringer?

Data og Netforsikring

Risikostyring kan udøves i større eller mindre omfang. Man skal blot have sig for øje, at det ikke er muligt fuldstændigt at forhindre konsekvenserne af it-relaterede risici, i hvert fald ikke uden enten store omkostninger eller uhensigtsmæssige arbejdsgange. Det kan derfor være relevant at tegne forsikring til dækning af uforudsete tab.

En Data- og Netforsikring forsikring består i princippet af to dele – en ansvarsdel og en første parts risiko.

Ansvarsdelen er den del, der omfatter det erstatningsansvar en virksomhed kan ifalde over for tredjemand, f.eks. pga. tab(bortkomst) af persondata eller fordi virksomheden har overført en virus til en anden virksomhed. Nye love og regler kræver, at man skal have ekstra sikkerhed, når man gemmer persondata, og det kræves samtidig, at virksomheden skal notificere alle, der er påvirket af et sikkerhedsbrud inden for 48 timer. Omkostninger til den slags notifikation dækkes af forsikringen.
Desuden dækkes også erstatningsbeløb, sagsomkostninger og forligsomkostninger, når der bliver rejst sag mod virksomheden med påstand om erstatning i sådanne sager.

Første parts delen omfatter de tab virksomheden selv lider. Det kan f.eks. være et driftstab i den periode, hvor virksomheden er "nede" pga. hackingen, kompensation for tab af indtægter, der ikke kan generes via internettet pga. forstyrrelser på internettet, som følge af hacking, eller udgifter til genetablering af data eller systemer efter hændelsen. Desuden kan forsikringen også dække det beløb virksomheden betaler, såfremt denne er udsat for "cyber"-afpresning, samt udgifter til PR firma, it-eksperter og advokatbistand.

Forsikringen er et produkt, som kan tilpasses virksomhedens behov, således man alene køber den dækning virksomheden har brug for. Willis kan, ved at undersøge virksomhedens nuværende forsikringer og virksomhedens risikobillede, yde rådgivning om hvilke dækninger, der er relevante for den konkrete virksomhed.

Kort om ledelsesansvar og forsikring

Såfremt nogen lider et økonomisk tab, som kan henføres til virksomhedens ledelses manglende stillingstagen til virksomhedens sikkerhedspolitik eller ledelsens manglende overblik og indsigt i virksomheden, kan denne/disse person(er) rette et krav mod ledelsen med påstand om erstatning.

Ledelsesansvar er det culpaansvar fysiske personer ifalder under udøvelsen af deres hverv som ledelsesmedlem, herunder bestyrelsesmedlem, direktør eller anden stilling med ledelsesbeføjelse.

Et ledelsesmedlem kan således ifalde erstatningsansvar både på baggrund af en handling og en undladelse, hvis disse samtidig har sammenhæng med det økonomiske tab modparten (f.eks. kreditorer, aktionærer m.m.) har lidt, samt at det var påregneligt for det skadevoldende ledelsesmedlem.

En ledelsesansvarsforsikring dækker krav rejst mod de sikrede ledere med påstand om ledelsesansvar i forbindelse med udøvelsen af deres ledelseshverv. En ledelsesansvarsforsikring indeholder en række undtagelser (og udvidelser), som typisk kan optimeres ved forhandling, så de tilpasses virksomhedens/ledelsens konkrete behov, både størrelses- og aktivitetsmæssigt samt geografisk.

Willis har i samarbejde med forsikringsselskaber udviklet særlige forsikringsbetingelser, der yder bredere dækning end sædvanligt, til fordel for Willis kunder.

Se mere på Willis side, særligt dediceret DVCA medlemmer: http://website.willis.dk/kompetencer-i-willis/boardroom-risk/finex-ledelsesansvar/dvca/

ksa@willis.dk

tio@willis.dk