E-business og Traditionel Forsikring

af **Aram Rowshangah**, Nordisk Commercial Udviklingschef, cand.merc.jur., Zurich
og **Lars Sørensen**, Senior Underwriter, cand.merc.jur., Zurich

Denne artikel belyser de særlige eksponeringer, der er relateret til E-business. Dette vil i stort omfang skabe nye forsikringsbehov, som de traditionelle forsikringer ikke tager højde for, hvilket både forsikringsbranchen samt virksomhederne skal være sig bevidst omkring.

Aram Rowshangah *Lars Sørensen*

Indledning

Den nye økonomi stormer frem, og E-business har allerede påvirket forretningsprocesserne i mange virksomheder, og det forventes at fortsætte med uformindsket styrke i de kommende år. Der er tale om en gigantisk vækst i E-business aktiviteterne i fremtiden, særligt indefor business-2-business området – fx estimerede Forrester Research medio 1997, at E-business handlen alene i USA ville blive USD 327 mia i 2002. I 1998 viste den globale E-business handel at være USD 301 mia. I dag antages business-2-business handlen om bare 3-5 år at nå USD 1.000 mia. på verdensplan.

Med andre ord skaber den nye økonomi helt nye muligheder for virksomhederne, men samtidig opstår der helt nye trusler og risici, som ikke nødvendigvis er dækket af de traditionelle forsikringer, der tilbydes på markedet. Det betyder, at forsikringsbranchen er nødt til at forstå de særlige risici, der er gældende for E-business aktiviteter således, at der kan udvikles forsikringsløsninger, der afspejler de risici, som dagens virksomheder står overfor.

Det er efterhånden næsten hver dag, at man kan læse i medierne om problemer i forbindelse med IT-sikkerhed, og det kan potentielt set ramme alle, som bruger de nye medier. Vi har allerede oplevet flere eksempler på omfanget af virusangreb såsom "I love you" virusen, som medførte tab for et 3-cifret USD millionbeløb.

E-business omfatter ikke alene virksomheder i den nye økonomi, men i særdeleshed også virksomheder i den gamle økonomi. Der findes vist næsten ingen virksomheder, der i dag ikke via sit edb-anlæg har adgang til internettet. E-business aktiviteten varierer lige

fra E-business virksomheden hvis hele koncept bygger på internettet til den lille service- eller handelsvirksomhed, der benytter e-mails og har en lille web-side, hvor virksomheden præsenteres. Alle virksomheder, der har forbindelse til internettet via fx e-mails eller hjemmearbjedspladser, har risici, der ikke nødvendigvis dækkes af de traditionelle forsikringer. Derfor er de mulige overvejelser vedrørende risicispørgsmål for E-business allerede i dag en aktuel problemstilling, som kræver opmærksomhed og fokus.

E-business eksponering

Et af de mulige risici, som virksomhederne er konfronteret med, er tyveri af data. Det kan både være ekstern hacking med henblik på at tilegne sig viden om nye produkter eller kundedata med det formål at afpresse virksomheden eller sælge informationen til konkurrenter, eller man kan såmænd også risikere at være udsat for intern hacking fra en utilfreds medarbejder. Dette kan medføre store omkostninger i form af genetablering af data, afpresning, tabt fortjeneste samt ikke mindst tabt omdømme i forhold til omverdenen, som kan gøre det vanskeligt at genskabe tilliden til virksomheden.

I den sammenhæng er det værd at bemærke, at hackerne i særdeleshed er blevet aktive de seneste år, og hackermiljøet er oftest på forkant med den teknologiske udvikling, hvorfor det kan være svært for virksomhederne at beskytte deres systemer mod angreb. Man bør ikke negligere det faktum, at hackerne har mulighed for at sløre deres identitet, og dermed kan det blive vanskeligt at finde kilden, så derfor skaber dette en yderligere udfordring for virksomhederne.

Alle virksomheder er sårbare overfor systemnedbrud, ikke mindst de virksomheder, som fx driver E-handel. Det er væsentligt at betone, at det ikke er et modefænomen, som udelukkende vedrører "dotcoms", men det er i langt højere grad virksomheder i den gamle økonomi, som på mange måder er mere etableret og velfunderet end de nye IT-virksomheder. Et godt eksempel kan være en bank, som pludselig udsættes for et systemnedbrud enten på grund af hacking, virus eller programmeringsfejl. Konsekvenserne kan være helt uoverskuelige i en her-og-nu betragtning, men omdømmet og risikoen for at miste kunder som følge af manglende troværdighed er de egentlige omkostninger, som skal tages i betragtning.

Et af de mulige problemer er programmeringsfejl, som kan opstå ubevidst på grund af en menneskelig fejl enten som følge af tastefejl eller manglende kendskab til og erfaring med virksomhedens IT-systemer. Konsekvensen af programmeringsfejl kan være, at virksomhedens firewalls "åbnes" for uautoriserede brugere, så der derved bliver adgang til virksomhedens kritiske data. En anden konsekvens kan meget vel være, at der ikke bliver adgang til systemet for autoriserede brugere, hvilket kan medføre tab i form af manglende transaktioner.

Virusangreb er en yderligere eksponering, som virksomhederne er konfronteret med. Det kan være fra eksterne kilder i form af e-mails o.l., hvor virus kan spredes til virksomheden enten bevidst eller ubevidst. Man kan også forestille sig, at der er tale om en intern kilde, hvis fx en ansat medbringer private programmer, som benyttes på arbejdspladsen, og hvor programmerne er inficeret med virus. Virus kan fx medføre datafejl, udsendelse af forkert information til kunder samt unødigt ressourcespild m.v.

Nye forsikringsbehov

På baggrund af ovenstående scenarier, bør virksomhederne tage højde for følgende eksponeringer i forbindelse med forsikringsdækningen:

- Driftstab som følge af systemnedbrud
- Ansvar som følge af systemnedbrud
- Intellectual property (Virksomhedens vidensdatabase)
- PR-omkostninger
- Cyberliability
- Electronic Publishing Liability (Informations-/formidlingsansvar)
- Extortion (Afpresning)

I relation til fx Intellectual Property er det værd at bemærke, at man har behov for at få dækket tabet for genfremstillings- samt udviklingsomkostninger, idet formler, forretningsstrategi o.l. er vitale for virksomhedens fremtidige drift, og disse kan være omkostningskrævende at genudvikle.

Hvis man er udsat for virus- eller hackerangreb og efterfølgende systemnedbrud, kan der være behov for at gøre brug af et PR-bureau med henblik på at bevare/genoprette tilliden til virksomheden, idet omdømmetabet kan vise sig at få alvorlige konsekvenser for virksomhedens fremtid.

Herudover kan man fx fremhæve forholdet vedrørende Electronic Publishing Liability, hvor man kan være udsat for krav fra 3. mand, hvis man fx lægger forkerte informationer ud på ens "web-site" med tab til følge. Dette kan fx være fejl i beregningsmodeller.

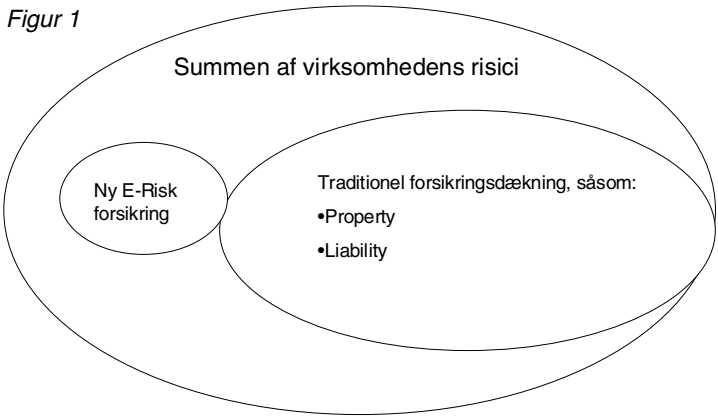
Endelig kan man udsættes for afpresning, ved at en hacker er kommet i besiddelse af kritisk information og truer virksomheden med at offentliggøre det eller videregive det til en konkurrent, medmindre der betales en løsesum. Her skal man tage højde for forhandlingsomkostninger og andre omkostninger i forbindelse med afpresningen.

Traditionelle forsikringer

I forhold til den ovenfor beskrevne redegørelse forekommer der et problem i forhold til de traditionelle forsikringer, når man betragter "trigger" og dækningsomfang. De traditionelle forsikringer er typisk kendetegnet ved, at der er sket en fysisk skade, hvilket ikke nødvendigvis er tilfældet ved E-business aktiviteter.

En traditionel propertyforsikring giver beskyttelse mod fysiske tab som følge af en dækningsberettiget begivenhed (se figur 1). Propertyforsikringen dækker derfor ikke som udgangspunkt skade, der skyldes virusangreb, og propertydækningen anerkender ikke i sin natur den eksisterende værdi af aktiver i elektronisk form, fx i relation til Intellectual Property. Ligeledes undtager man dækning for menneskelige programmeringsfejl, selv om risikoen så absolut er tilstede.

Figur 1



Den traditionelle erhvervsansvarsforsikring bygger på forudsætningen om, at der skal være indtruffet en fysisk skade på 3. mand, hvilket ikke nødvendigvis er samstemmende med den risiko, som er forbundet med at drive E-business,

idet det ikke er den fysiske skade, som tiltrækker sig opmærksomheden men snarere de økonomiske følger for virksomheden og dennes samarbejdspartnere.

Kriminalitetsforsikringen er udviklet til at dække økonomiske tab, men der gives normalt ikke dækning for virksomhedens eget driftstab ved en skade, og man tager heller ikke i dette tilfælde højde for værdien i relation til Intellectual Property. Ligeledes negligeres behovet for dækning af eksterne PR-aktiviteter i tilfælde af en skade på trods af, at virksomheden tillægger dette stor betydning.

Afslutning

Der er ingen tvivl om, at virksomhederne er eksponeret for større risici, end de traditionelle forsikringer afdækker. Det er derfor nødvendigt, at forsikringsmarkedet i større omfang end hidtil tager dette alvorligt og medvirker til at afhjælpe virksomhedens risici. En væsentlig opgave i denne proces er, at man skal forstå eksponeringen i relation til E-business, og når dette er gjort, må man nødvendigvis vurdere, hvorledes man vil håndtere eksponeringen.