Willis Towers Watson
Cyber forsikring og risikostyring

Sikkerhed & Revision 2016

Willis Towers Watson

Kort om Willis Towers Watson

- En organisation med rødder tilbage til 1828
- Omsætning på omkring USD 8B
- Total set 39,000 ansatte
- Lokal tilstedeværelse I 131 lande – det største netværk af Riskorådgivere.
- Fire forretningsområder
  - Corporate Risk and Broking
  - Human Capital and Benefits
  - Investment, Risk and Reinsurance
  - Exchange Solutions

- Partnerejet i Danmark siden 1984
- Omsætning på mere end DKK 500M
- Omkring 450 ansatte
- 5 kontorer: Nærum, Odense, Aarhus, Holstebro og Aalborg

Indhold

1. Mega trends
2. Risikostyring fra vores perspektiv
3. Willis Towers Watson Risk Indicator
4. Cyberforsikring samt faldgrupperne i forsikringsdækning
5. Cyberforsikring vs kriminalitetsforsikring
6. Afslutning og spørgsmål

MEGA trends?

It-kriminalitet

- Hacking
- Spionage/overvågning/IPR
- Pengeoverførsel/Bedrageri

Lovgivning

- Dataklassifikation
- Sanktioner
- Kontrakter

Risikostyring

- Awareness
- Operationel & Strategisk risikostyring
- Ressourcefordeling

Cyber risici – hvad taler vi om?

Hvilke hændelser betegnes typisk som cyberrisici inden for forsikring og hvilke konsekvenser kan det eksempelvis have?

- **Databrud**
- **Hacking**
- **Malware/Virus**
- **Ransomeware angreb**
- **Ddos-angreb**
- **Virustransmission til tredjemand**
- **Ansattes sabotage**
- **Ændring af indhold på diverse medier**
- **Betjeningsfejl**
- **Systemnedbrud (som følge af angreb)**

De beskrevne cyberhændelser / angrebstyper kan have forskellige konsekvenser for virksomheden:

F.eks. vil et databrud kunne betyde, at fortrolig information om ansatte, kunder eller tredjeparts virksomheder offentliggøres uberettiget eller at det anvendes til at afpresse organisationen.

F.eks. Kan et Ddos angreb (distributed denial of service) medføre et driftstab eller at organisationen ikke kan levere den normale service.

Alle hændelserne vil kunne medføre et økonomisk tab, enten i form af erstatningsbeløb eller omkostninger til at håndtere hændelsen

Eksempler

Eksempel 1: Ransomewareangreb

Postnord fil – Pakkelevering.

Firewalls + spamfiltre fangede mailen i outlook, men medarbejderen havde adgang til privat yahoo-mail på arbejdspc også.

Kryptering af 1000 filer inden for 3 timer.

Eksempel 2:

Organisationen gjorde brug af it-leverandør. Systemfejl hos dem betød 1 dags nedetid. Tabet er opgjort til ca. 8 -10 mio. kr.

Eksempel 3:

Fake president fraud.

E-mail korrespondance + adgang til systemet.

Overførsel af midler til ”hemmelig” transaktion.

Eksempel 4:

Hacking af system + bogføring

Nye afregninger eller ændrede kontonumre.

Eksempel 5:

Industrispionage.

Hackere var i virksomhedens system i min. 6 mdr.

Det tog 3 måneder, at ”lukke” dem ned.

Persondata - EU-Forordning

Væsentlige punkter i den nye forordning:

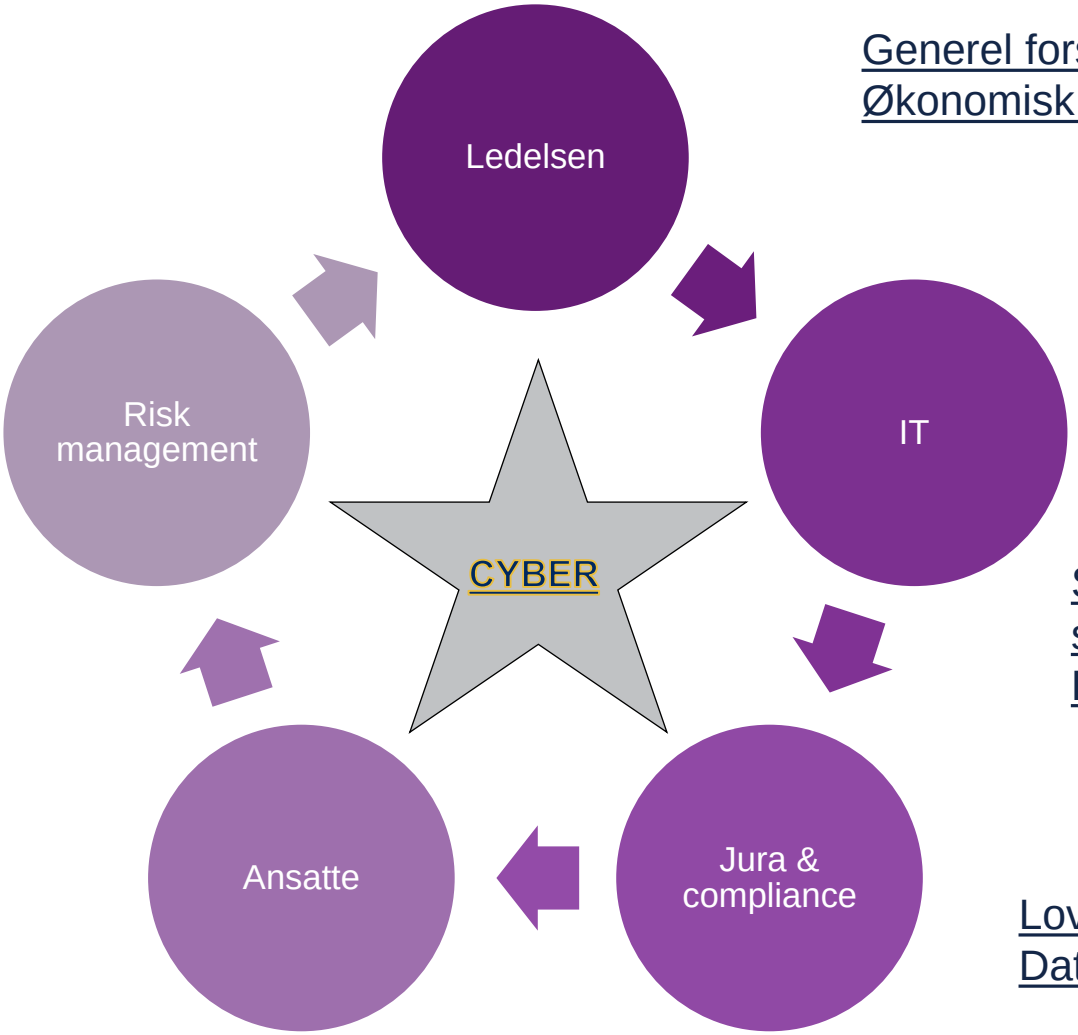
Der er i 2016 opnået enighed om den fulde ordlyd af EU persondataforordningen.

Dette betyder, at forordningen formelt vil træde i kraft 25. maj 2018.
Den 2 årige frist for ikrafttrædelsen betyder, at forordningen først vil få virkning for alle berørte virksomheder og myndigheder 2 år efter vedtagelsen.

Nedenfor er en kort opsummering af nogle af de væsentlige punkter i forordningen, som virksomheder og myndigheder bør have fokus på.

- **Krav til dokumentation**
- **Der er indført en ret til at blive glemt (right-to-be-forgotten)**
- **Notifikation til datatilsynet og berørte personer**
- **Data Protection officer i offentlige myndigheder og visse private virksomheder**
- **”One-stop-shop”**
- **Sanktioner – væsentligt forhøjet bødeniveau**

Risikostyrings elementer



Generel forståelse
Økonomisk forståelse

Kontrol
Forsikring
CISO

Software
sikkerhed
Beredskabsplan

Awareness
Træning

Lovgivning
Data

Spørgsmål til afdækning af risikoen

1. **Dataklassifikation:** Er der foretaget en opstilling af forretningskritiske data i prioriteret rækkefølge?
2. **Beskyttelse/backup:** Hvordan beskyttes disse informationer? Tages der højde for forskellige niveauer af fortrolighed?
3. **Databrud:** Hvad er konsekvenser og tab hvis disse informationer kompromitteres eller uberettiget/utilsigtet offentliggøres?
4. **Sikkerhedspolitik:** Formuleret? Herunder; er den implementeret, opdateret og testet?
5. **Medarbejdertræning:** Træning i at overholde politikken? og hvordan sikres det at de arbejder ud fra retningslinjerne heri? Sikkerhedskultur?
6. **Strategi:** Er sikkerhedstiltagene forankret i ledelsen?
7. **Beredskab:** Er der et beredskab ved cyber hændelser, der indebærer IT, jura, økonomi, kommunikation inklusive aftaler med rådgivere?
8. **Trusler:** Hvem kan formodes at angribe? Hvad er deres motiver, metoder, placering mm.?
9. **Samarbejdspartnere/kontrakter:** Drøftelse med samarbejdspartnere, outsourcing partnere om deres sikkerhed, beredskab mm. /ansvar i kontrakter?
10. **Jurisdiktion** i forhold til ansvar? Overholdelse af Persondataloven?

Tegn jeres organisations eget risikobillede og få styr på jeres beredskabsprocedurer!

- Hvad er organisationens specifikke risiko?
- Hvor er I mest sårbare? Kan organisationens bundlinje påvirkes af et cyberangreb? Og i hvor høj grad?
- Er der styr på jeres backup procedurer samt beredskabsprocesser ?
- Hvem gør hvad, hvornår?

Skadeshåndtering

Opdagelse

Aktuelt eller formodet brud, tyveri, uberettiget offentliggørelse eller misbrug af fortrolig information.

Anmeldes til forsikringsselskab/krise-konsulent

Respons

Kriseberedskab skal iværksættes:

- It-konsulenter (Forensic)
- Juridisk assistance
- PR/mediedækning
- Notifikation
- Tabsbegrænsning
- Genopretning/genetablering

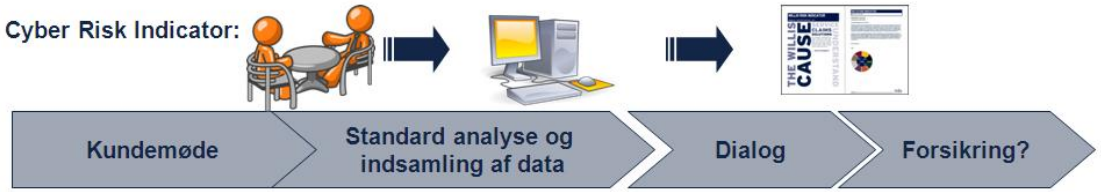
Konsekvenser

Uden korrekt håndtering af en krise, kan virksomheden risikere:

- Driftstab
- Skade på renommé eller ”brand”
- Erstatningskrav
- Sanktioner fra myndigheder
- Tab af kunder/forretningsforbindelser

Hvordan analyserer Willis Towers Watson risikoen hos organisationer?

- Risk Indicator



NIVEAU I:

Willis Cyber Risk Indicator (WCRI) er baseret på et grundlæggende niveau, hvor oplysninger og informationer indsamles, gennemses og vurderes med henblik på skabe overblik over organisationens grundlæggende sikkerhedsniveau.

- Risikointerview
- Risikoanalyse
- Drøftelse af risiko og forsikringsmuligheder

Hvilken dækning indebærer en typisk cyberforsikring

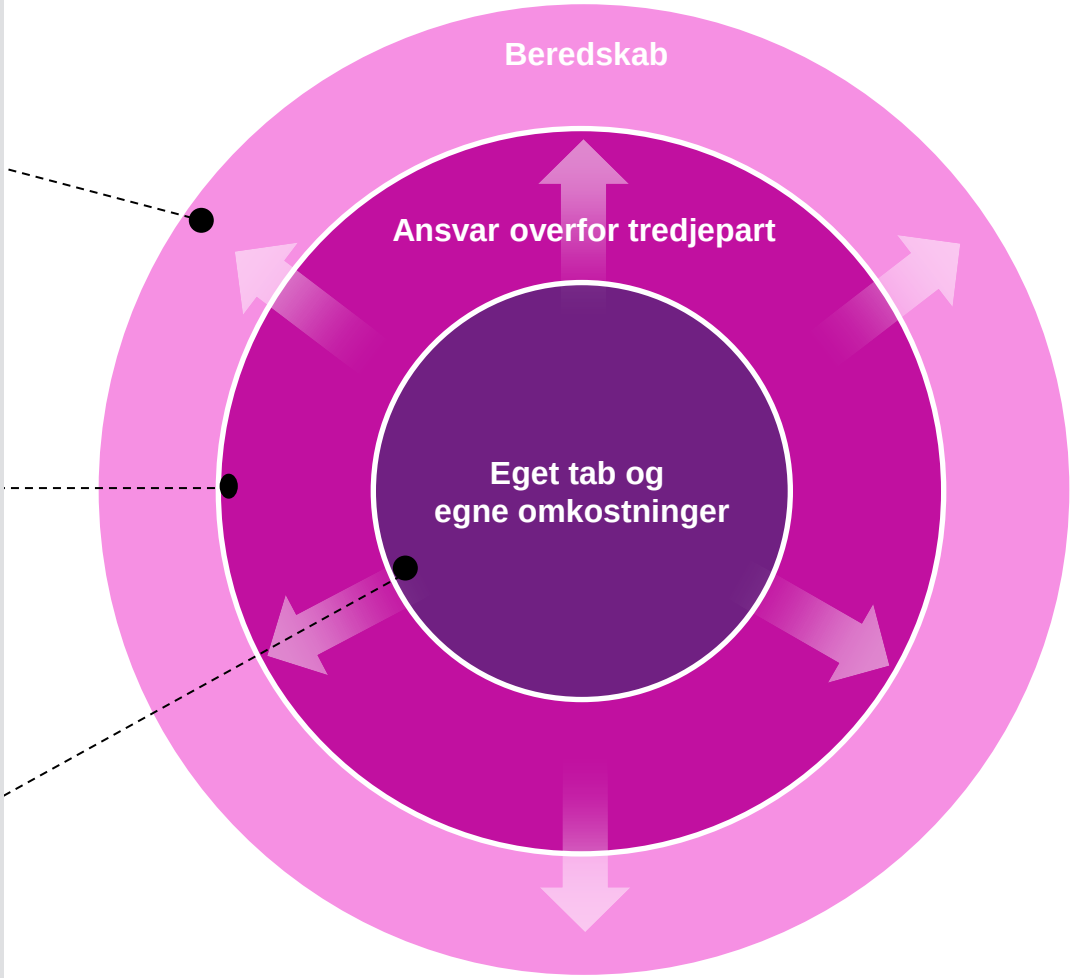
Beredskab
- Nogle forsikringsselskaber tilbyder en hotline til et beredskab. Andre dækker omkostninger. Begge dele indebærer dækning af følgende:

- Omkostninger til IT-konsulenter
- Omkostninger til Advokater
- Omkostninger til PR konsulenter

Ansvar overfor trejdepart
- Erstatningsansvar (f.eks. ved brud på persondatalovgivning)
- Underretningsomkostninger
- Erstatningskrav som følge af videreførsel af virus /malware
- Krænkelser (frihed, ærge, dårlig omtale)
- Uberettiget deep-linking på hjemmeside
- Sanktioner (f.eks. Bøder af myndigheder)
- Erstatningskrav som følge af manglende levering

Egne omkostninger
- Driftstab / indtægtstab
- Direkte tab af data eller penge

- <u>It-konsulentomkostninger som følgende:</u>
  - Undersøgelse af omfanget af et angreb
  - Dekryptering af filer / Fjernelse af virus
  - Løsesum / forhandling
  - Genetablering af data / systemer / netværk
  - Meromkostninger
  - Bevissikring



Faldgrupper i forsikring

Hvad skal man være særligt opmærksom på?

- Dækningsomfanget
- Hvad udløser forsikringsdækning? ”Insurance Trigger”
- Undtagelser?
- Outsource service provider / cloud-løsning /it-leverandør?
- Driftstabsdækningens rækkevidde? – Hvordan beregnes dit driftstab?
- Særlige behov i forhold til kontrakter med samarbejdspartnere/kunder.

Cyberforsikring vs kriminalitetsforsikring

Begivenhed	CRIME	CYBER
Ansattes bedrageri, tyveri, underslæb, mandatsvig	+	÷
Sikredes erstatningsansvar overfor tredjemand (pga. ansattes bedrageri)	+	÷
Netbankindbrud	+	÷
Fysisk beskadigelse af løsøre	+	÷
Elektronisk afpresning	Delvist (undersum)	+
Tab af data (genetableringsomkostninger)	Delvist (undersum)	+
Tab af data (erstatningsansvar)	÷	+
Fjernelse af virus, malware, kryptering og genetablering af netværk	Delvist (undersum)	+
Driftstab / Meromkostninger	÷	+
Omkostninger til it-konsulenter	÷	+
Advokatomkostninger	÷	+

‘*Dette er baseret på en vurdering af hvad almindelige CRIME OG CYBER forsikringer dækker. Der kan være særlige forhold I den enkelte police.

Afslutning og spørgsmål

Spørg løs!

Hvor kan du få mere viden om cyberrisici?

www.cyberrisk.dk

Tine Olsen
Practice Leader FINEX, Willis Specialties Practice,
Cand. Jur., HD(O)

D +45 88139431
M +45 29213810

tine.olsen@willistowerswatson.com