# Zes onderdelen die Data Risk dekking omvatten

1. **Systeeminbraak**:
Deze dekking dekt eigen kosten als gevolg van inbraak op systemen of data:

- kosten van forensisch onderzoek.
- kosten van communicatie met klanten, toezichthouders, justitie, creditmaatschappijen en andere belanghebbenden.
- kosten voor extra klantenondersteuning, bijvoorbeeld via een call centre.
- kosten van crisismanagement, reputatieherstel en pr-campagnes.

2. **Privacy**:
Deze dekking dekt gevolgen van gestolen privacygevoelige gegevens:

- kosten van onderzoek door bijvoorbeeld justitie of creditcardmaatschappijen.
- claims van individuele personen.
- boetes opgelegd door toezichthouders, of andere verplichte vergoedingen.

3. **Digitale aansprakelijkheid**:
Deze dekking dekt voortvloeiende schade als bijvoorbeeld de website of e-mail onbedoeld het auteursrecht schendt, laster verspreidt of een virus bevat.

4. **Hacking**:
Deze dekking dekt de schade veroorzaakt door hackers:

- reparatie, vervanging of herstel van websites, programma's of data.
- kosten van gestolen software of data.
- kosten van onderzoek en advies in systeembeveiliging.
- kosten van forensisch onderzoek naar de oorzaak van een hacking.

5. **Afpersing**: beschermt uw relatie tegen de schade van hackers die de website of data gijzelen. Uw relatie krijgt bijstand van security-adviesbureau NetDiligence en eventueel betaald losgeld wordt vergoed.

6. **Omzet verlies door cyberaanvallen**: dekt omzetverlies door bijvoorbeeld een DDos-actie of andere aanval op de computersystemen van uw relatie, leidt tot omzetverlies, bijvoorbeeld door uitval van een webwinkel

*Alle onderdelen zijn in één pakket verzekerd. Het is niet mogelijk om de onderdelen los van elkaar te verzekeren.*