

**B**ij Vanbreda Risk & Benefits stellen we vast dat bedrijven steeds vaker een cyberpolis afsluiten door groeiende digitale bedreigingen en toenemende afhankelijkheid van technologie. In een tijdperk waarin bedrijfsprocessen, communicatie en gegevensopslag grotendeels gedigitaliseerd zijn, worden ondernemingen kwetsbaarder voor cyberaanvallen. Een cyberpolis biedt financiële bescherming en dekt de schade die kan ontstaan door datalekken, ransomware-aanvallen, ...

### Ransomware-aanvallen kunnen je bedrijf langdurig gijzelen

Waar de fysieke diefstallen dalen, swingen digitale diefstallen door cybercriminelen de pan uit. Zo'n crimineel gaat op zoek naar de waardevolle informatie die bedrijven bezitten. Hij probeert de info te stelen of versleutelt je systemen voor financieel gewin. Een bedrijf langdurig digitaal gijzelen door een ransomware-aanval? Het gebeurt vaker dan je denkt.

### Kies voor de gemoedsrust van een cyberverzekering

Een cyberpolis is een onmisbaar deel van je bedrijfsstrategie om je zo goed mogelijk te beschermen tegen cybercriminaliteit. De ideale cyberpolis bestaat uit drie luiken.

- Het eerste luik is een vergoeding van alle eigen schade bij zo'n aanval. Denk daarbij aan de herstellkosten, de honoraria van alle experts, het verlies van inkomsten tijdens de onderbreking van je bedrijfsactiviteit tot zelfs het te betalen losgeld.
- Een tweede luik is de financiële schade die je aan derden berokkent door de cyberaanval.
- En het laatste luik is de hulplijn waarop je een beroep kan doen. Dit houdt onmiddellijke ondersteuning in bij een cyberincident door IT-, PR-, legal- en crisisexperten. Voor vele bedrijven is dit het meest waardevolle aspect van de cyberverzekering, aangezien je de schade van een cyberincident zeer sterk kan beperken door snel en adequaat in te grijpen.

### 90% van de cyberincidenten wordt veroorzaakt door een menselijke fout

Een cyberpolis maakt deel uit van je risicomanagement, net zoals preventie. Zo stellen we vast dat 90% van alle cyberincidenten steeds start bij een menselijke fout. Voorbeeld: een medewerker klikt op een corrupte link, downloadt een corrupt bestand, ... en de poppen gaan aan het dansen. Het

is cruciaal om je medewerkers attent te maken op de verschillende cyberrisico's en hen te leren hiermee correct om te gaan. Dit kan je doen via phishing-simulaties, online training of andere workshops.

### Dienstverlening Vanbreda Risk & Benefits

Wij ondersteunen onze klanten in de zoektocht naar de juiste verzekeringen en helpen we hen bij het creëren van bewustwording bij werknemers. Zo bouwen we samen met onze klanten aan hun 'human firewall'!

Deze expertise werd aangeboden door:

**Vanbreda Risk & Benefits**  
— [vanbreda.be](http://vanbreda.be)



### Waarom sluiten bedrijven steeds vaker een cyberpolis af?

Beantwoord door Jonas Mannaerts en Steven Dierckx van Vanbreda.