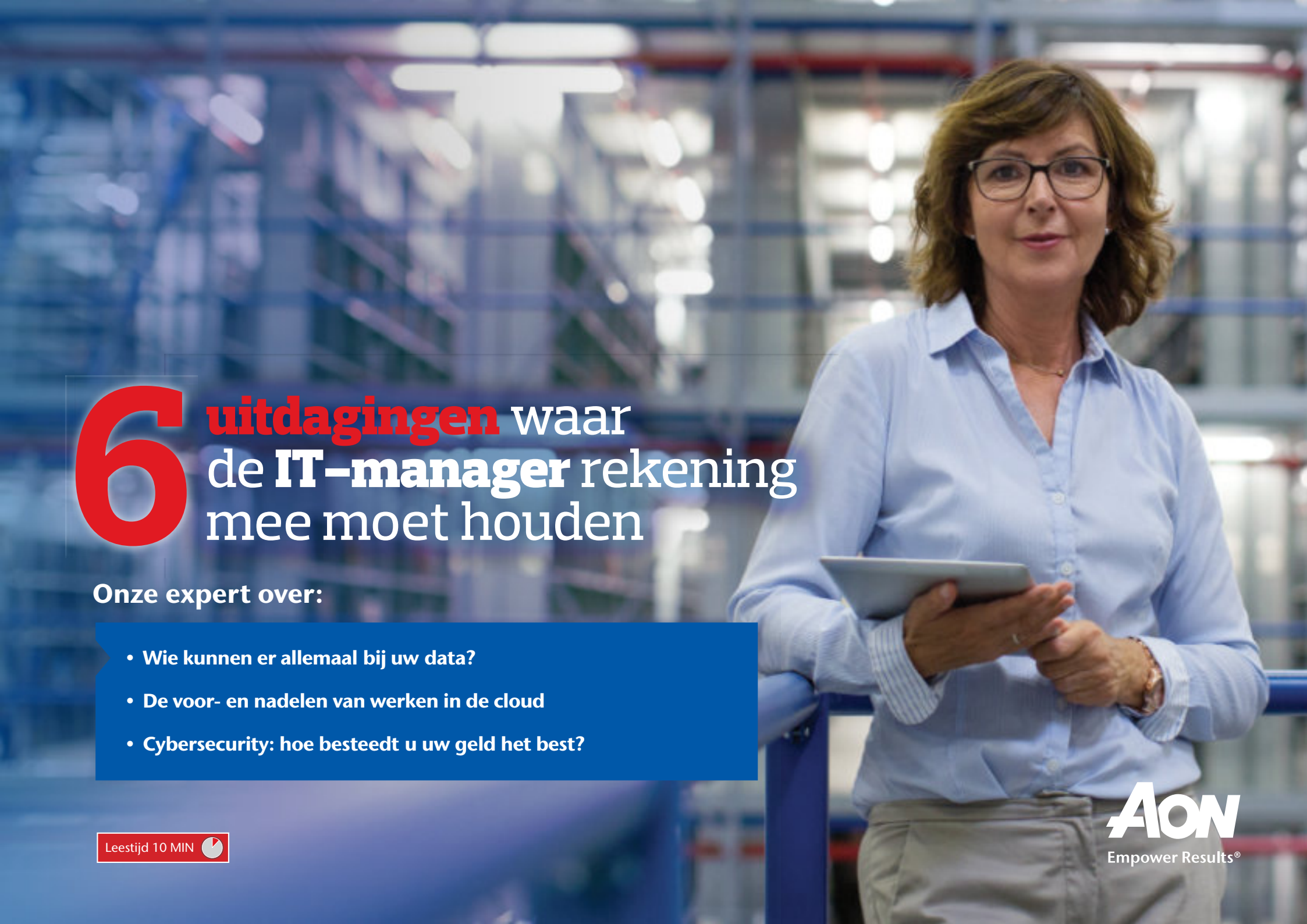


6 uitdagingen waar de IT-manager rekening mee moet houden

Onze expert over:

- Wie kunnen er allemaal bij uw data?
- De voor- en nadelen van werken in de cloud
- Cybersecurity: hoe besteedt u uw geld het best?

Leestijd 10 MIN

AON
Empower Results®

Continuïteit in een **turbulente periode**

Van de handelsoorlog tussen de Verenigde Staten en China tot aan de ongekende recessie waarin we onvermijdelijk terechtkomen: de geopolitieke ontwikkelingen beïnvloeden de wijze waarop wij ons leven en onze samenleving inrichten.
Voor bedrijven is het zaak om in zo'n turbulente periode de continuïteit te waarborgen. Ze moeten zo wendbaar en adaptief mogelijk zijn. Als IT-manager levert u daar een bijdrage aan door optimaal gebruik te maken van digitalisering. Digitalisering levert echter een aantal grote uitdagingen op. Wij hebben zes uitdagingen op een rij gezet om als IT-manager rekening mee te houden.

6 uitdagingen waar de IT-manager rekening mee moet houden

AON
Empower Results®

Wie kunnen er allemaal bij **uw data**?

Om de concurrentie voor te blijven is het noodzakelijk om mee te gaan in ontwikkelingen die met risico's gepaard gaan. Zo is het steeds normaler om klanten en leveranciers toegang te verlenen tot een portal die gekoppeld is aan de interne systemen van uw bedrijf. Hoewel alle betrokken partijen daar baat bij hebben, levert het ook een risico op: het maakt uw data mogelijk kwetsbaar en toegankelijk voor ongeautoriseerden. Uw bedrijf heeft de zorgplicht om alle data die u verzamelt zorgvuldig te verwerken en te bewaren.

U heeft dus te maken met een spanningsveld van mogelijkheden en beperkingen. Er wordt van u als IT-manager verwacht dat de digitale systemen de organisatie maximaal vooruithelpen. Tegelijkertijd bent u verantwoordelijk voor de veiligheid van deze systemen en de data. U vervult in deze complexe situatie een strategische rol. Hoe gaat u om met deze dynamiek?

AON
Empower Results®

De **voor- en nadelen** van werken in de **cloud**

Het is van essentieel belang om te luisteren naar de behoeftes van de medewerkers en de directie. Welke keuze maakt u bijvoorbeeld met betrekking tot de opslag van het intellectuele eigendom van uw bedrijf? Kiest u ervoor om dit in eigen beheer te doen of bewaart u de data in de cloud? Uw keuze hangt af van factoren die voor uw bedrijf belangrijk zijn: zijn uw gegevens altijd direct beschikbaar, hoe zit het met de integriteit van uw gegevens, en beschikt u over back-ups om de continuïteit van uw bedrijf te waarborgen? Voor iedere keuze is draagvlak nodig. Daarom is het noodzakelijk om te kunnen beargumenteren waarom een gekozen oplossing uw voorkeur heeft.

Het is dus van belang om steeds uit te gaan van het doel dat u wilt bereiken. Is het voor uw bedrijf nodig om dynamisch te zijn en snel te kunnen op- en afschalen? Dan lijkt de cloud de ideale oplossing. Als u daarvoor kiest, is het belangrijk duidelijk afspraken te maken over hoe gevoelige data wordt afgeschermd, zowel voor externen als voor medewerkers. Kiest uw organisatie liever voor opslag in eigen beheer? Dan is het de vraag hoe afhankelijk u wilt worden van een externe partij die de serverruimte verschaft of hoe u uw eigen serverruimte aan de minimale eisen laat voldoen.

AON
Empower Results®

De **juridische** kant van de zaak

Overigens is de afscherming van data niet alleen een technische zaak. Juridische vereisten spelen hierbij ook een rol. Zeker de laatste jaren is het databeleid van bedrijven onder een vergrootglas komen te liggen: de wet- en regelgeving is strenger geworden waardoor u hogere eisen stelt aan uw partners en leveranciers. Het is daarom zaak om heldere afspraken te maken met deze partijen. Ook de eindklant is door de jaren heen steeds kritischer en mondiger geworden.

Meer dan ooit werkt de IT-manager samen met de legal counsel om de juridische kant van de zaak op orde te brengen. **Een legal counsel helpt u heldere afspraken op papier te zetten:** wat verwacht u van de aanbieder, hoe lang duurt de samenwerking en wie is er verantwoordelijk als er iets misgaat? Zijn de afspraken met de klant helder, welke bevoegdheden krijgt u van uw klanten en hoe gaat u goed met hun gegevens om?

Cybersecurity: hoe besteedt u uw geld het best?

U maakt dus een voortdurende afweging tussen optimalisatie en veiligheid. In alle lagen van de organisatie wilt u over de beste technische oplossingen beschikken, op voorwaarde dat de security geborgd is. Dat is een complexe klus, zeker gezien de groeiende cybercriminaliteit. Het Cyber Security Risk Report 2020 beschrijft cybersecurity als een puzzel die een oplossing biedt door op de juiste manier met alle puzzelstukken om te gaan.

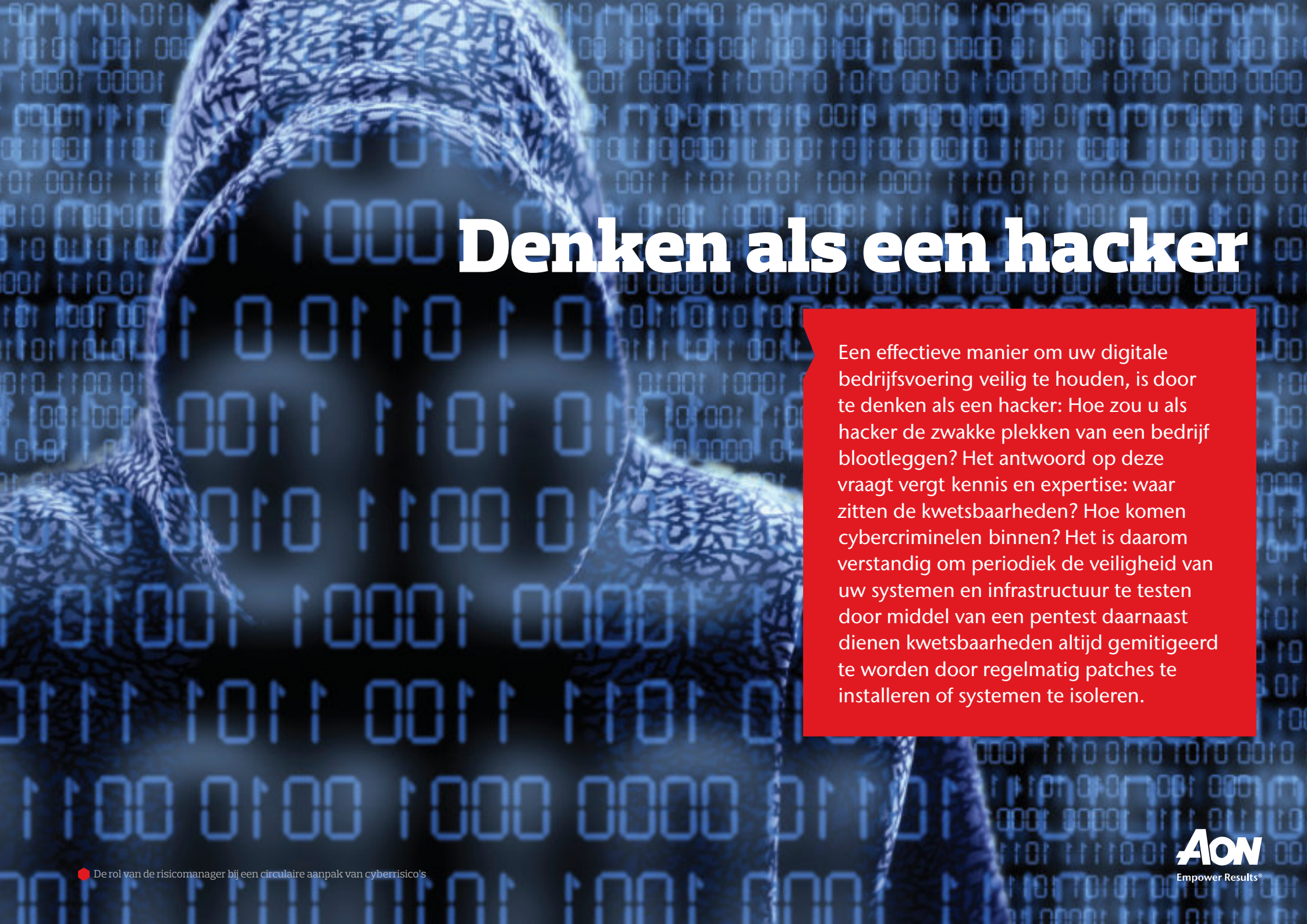
De omgang met intellectueel eigendom, zoals copyrights, datarechten en bedrijfsgeheimen, is een fundamenteel onderwerp voor de IT-manager om aandacht aan te besteden. Diefstal van vertrouwelijke bedrijfsinformatie richt wereldwijd zo'n 1 biljoen dollar schade aan. Daarnaast worden bedrijven in toenemende mate het slachtoffer van digitale fraudeurs, die medewerkers met behulp van ransomware afpersen. Ook wanneer uw bedrijf een ander bedrijf overneemt, bent u mogelijk vatbaar voor cybercriminaliteit.

Wanneer ook op IT-vlak synergie plaatsvindt, kunnen onbedoeld kwetsbaarheden in de IT-organisatie van het overgenomen bedrijf ook uw bedrijf raken.

Jaarlijks investeren bedrijven wereldwijd 600 miljard euro in cybersecurity. Om uw beschikbare budget effectief in te zetten, voert u een businessimpactanalyse en een strategische risicoassessment uit. Daarmee identificeert u de kroonjuwelen met onderliggende IT-systemen om de kwetsbaarheid en afhankelijkheid van uw organisatie in kaart te brengen. Zo bepaalt u welke technische en organisatorische maatregelen nodig zijn om de veiligheid en continuïteit naar het gewenste niveau te krijgen.

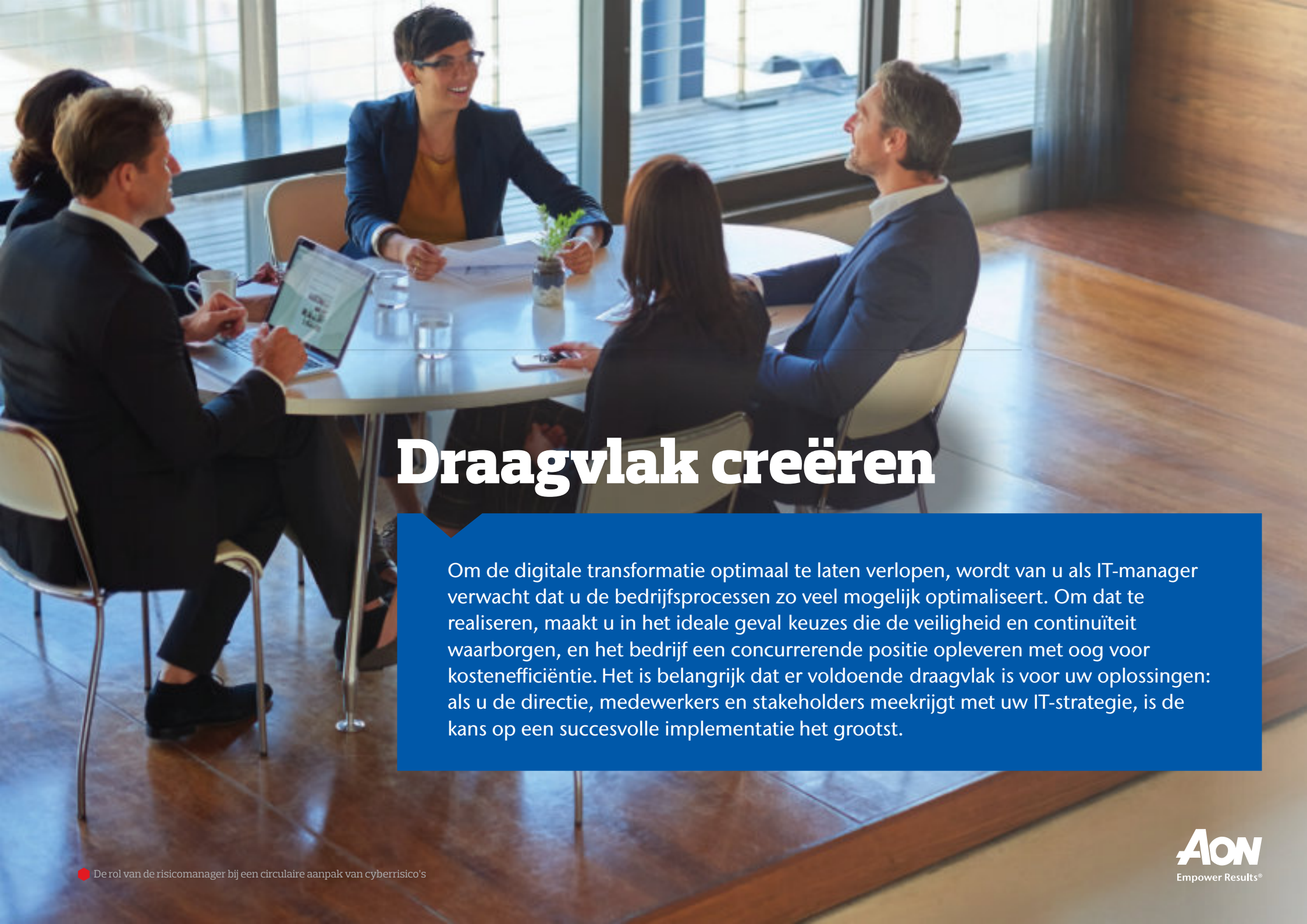
De rol van de risicomanager bij een circulaire aanpak van cyberrisico's

AON
Empower Results®



Denken als een hacker

Een effectieve manier om uw digitale bedrijfsvoering veilig te houden, is door te denken als een hacker: Hoe zou u als hacker de zwakke plekken van een bedrijf blootleggen? Het antwoord op deze vraagt vergt kennis en expertise: waar zitten de kwetsbaarheden? Hoe komen cybercriminelen binnen? Het is daarom verstandig om periodiek de veiligheid van uw systemen en infrastructuur te testen door middel van een pentest daarnaast dienen kwetsbaarheden altijd gemitigeerd te worden door regelmatig patches te installeren of systemen te isoleren.



Draagvlak creëren

Om de digitale transformatie optimaal te laten verlopen, wordt van u als IT-manager verwacht dat u de bedrijfsprocessen zo veel mogelijk optimaliseert. Om dat te realiseren, maakt u in het ideale geval keuzes die de veiligheid en continuïteit waarborgen, en het bedrijf een concurrerende positie opleveren met oog voor kostenefficiëntie. Het is belangrijk dat er voldoende draagvlak is voor uw oplossingen: als u de directie, medewerkers en stakeholders meekrijgt met uw IT-strategie, is de kans op een succesvolle implementatie het grootst.

Aan de slag met de digitale transformatie

Wilt u de digitale transformatie van uw bedrijf veilig laten verlopen? Aon's specialisten helpen u in elke fase van het proces met advies op maat.

Ralf Willems
+31 (0)10 448 77 72
ralf.willems@aon.nl

Aon
Empower Results®