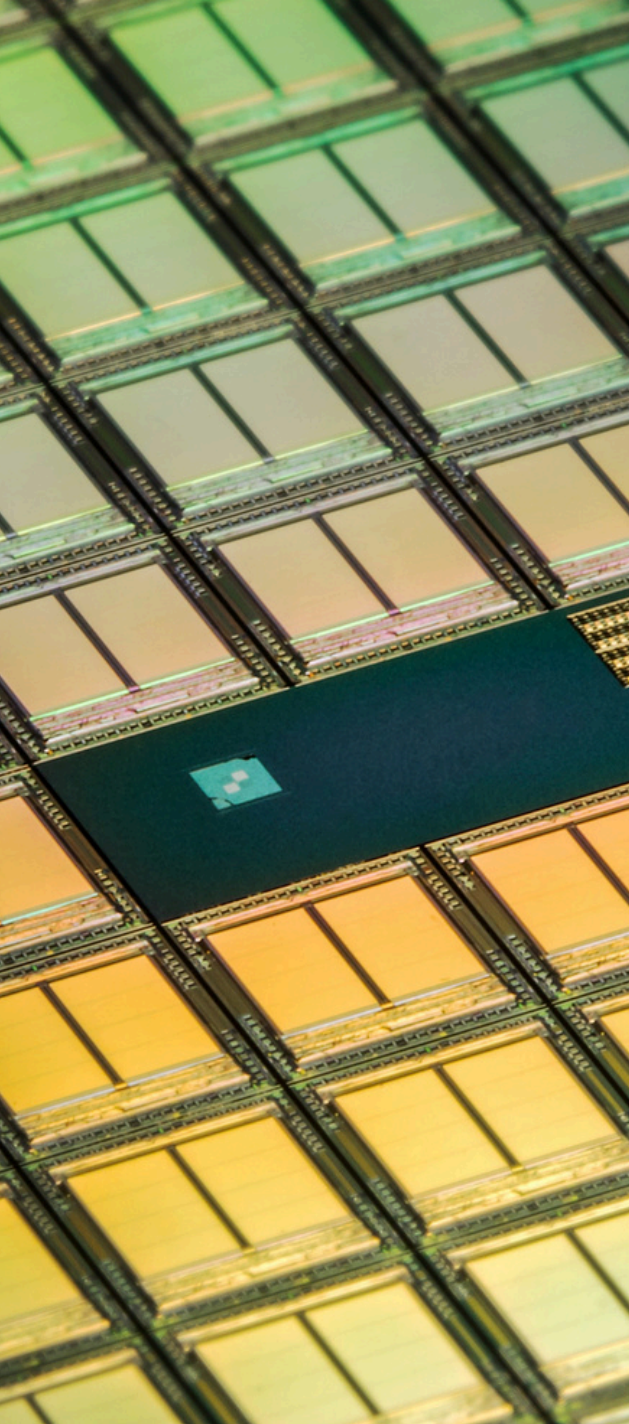


# Wat als morgen jouw productie stilvalt?

Hoe bescherm je jouw productie, OT en supply chain en wat vraagt NIS2 van jouw organisatie?

**HOWDEN**



# Digitalisering maakt de maakindustrie slimmer én kwetsbaarder

Machines, OT-systemen, ERP-software, leveranciers en medewerkers zijn steeds sterker digitaal verbonden. Dat helpt je slimmer, sneller en efficiënter produceren maar het maakt je productie ook afhankelijker van technologie.

Valt een digitaal systeem uit, dan kan de impact direct voelbaar zijn op de werkvloer. Een cyberincident kan de productie vertragen of stilleggen, leveringen raken en gevoelige bedrijfsinformatie blootleggen. Goed inzicht in die afhankelijkheden helpt je om bij een incident sneller te handelen en de impact te beperken.

## Bijna 20% industriële computers

Op 19,6% van de door Kaspersky gemonitorde industriële computers werd in het eerste kwartaal van 2026 een cyberdreiging gedetecteerd en geblokkeerd. In de maakindustrie nam dit percentage als enige sector toe.

Bron: Kaspersky ICS CERT, Q1 2026

## Slechts 19% van de bedrijven

19% van alle Nederlandse bedrijven is verzekerd voor cybersecurityincidenten. Grotere bedrijven zijn dit vaker dan kleinere organisaties.

Bron: CBS, Cybersecuritymonitor 2025

## NIS2 is van kracht

Sinds 15 augustus 2026 geldt de Cyberbeveiligingswet. Valt je organisatie eronder, dan gelden concrete eisen voor het beheersen en melden van cyberrisico's. Ook leveranciers kunnen via hun klanten met strengere eisen te maken krijgen.

Bron: Rijksoverheid / RDI / NCSC

# Cyber stopt niet bij IT

Een cyberaanval hoeft je machines niet rechtstreeks te raken om je productie stil te leggen. Als je planning niet beschikbaar is, een leverancier uitvalt of medewerkers geen toegang meer hebben tot kritieke systemen, kan de impact al snel op de werkvloer voelbaar zijn. En terwijl de productie misschien gewoon doordraait, kunnen ondertussen waardevolle ontwerpen of productdata worden buitgemaakt.

Cyber risico kent verschillende routes. Dit zijn vier scenario's die voor maakbedrijven grote gevolgen kunnen hebben.



## 1. Een aanval bereikt je productieomgeving

Via een slecht beveiligde verbinding, besmette laptop of externe onderhoudspartij krijgen aanvallers toegang tot de OT-omgeving. Ze kunnen systemen verstoren die machines of productielijnen aansturen of bewaken. Soms wordt de productie uit voorzorg stilgelegd omdat het niet meer zeker is dat machines veilig en betrouwbaar functioneren.



**Gevolg:** productiestilstand, herstelkosten en mogelijk risico voor kwaliteit of veiligheid.



## 2. Ransomware blokkeert je bedrijfsvoering

Een medewerker klikt op een overtuigende phishingmail of aanvallers misbruiken een kwetsbaarheid in software. Ze krijgen toegang tot het netwerk en versleutelen bijvoorbeeld je ERP-, plannings- of voorraadsysteem. Machines zijn misschien nog operationeel, maar orders, materiaal informatie of productieplanningen zijn niet meer beschikbaar.



**Gevolg:** productie loopt vertraging op of valt stil terwijl IT-specialisten systemen onderzoeken en herstellen.



## 3. Een cyberincident bij een leverancier raakt ook jou

Je productie kan afhankelijk zijn van software in de cloud, een IT-dienstverlener of een leverancier die op afstand machines onderhoudt. Wordt zo'n partij getroffen door ransomware of valt een belangrijke digitale dienst uit, dan kun jij bijvoorbeeld niet meer plannen, produceren of uitleveren.



**Gevolg:** productie-verstoring door een incident buiten je eigen organisatie.



## 4. Eigendomsrechten en kennis komen in verkeerde handen

Ontwerpen, technische specificaties, productdata en prijsinformatie vertegenwoordigen grote waarde. Worden deze gegevens gestolen, dan kan dat je concurrentiepositie, financiën en reputatie raken.



**Gevolg:** verlies van kennis, concurrentievoordeel en klantvertrouwen.

# Lever je aan defensie? Dan kan ook je cyberrisico veranderen

Maakbedrijven die direct of indirect leveren aan defensie, dual-use toepassingen of andere strategische sectoren kunnen met andere cyberdreigingen te maken krijgen. Niet alleen je systemen, maar ook technische kennis, ontwerpen en je positie in de keten kunnen waardevol zijn voor aanvallers.

Cyberrisico gaat dan verder dan ransomware en financiële criminaliteit. Ook digitale spionage, diefstal van hoogwaardige technologie en doelbewuste verstoring vragen om aandacht. De AIVD waarschuwt dat onder meer Nederlandse topsectoren en de defensie-industrie een verhoogd risico lopen op digitale spionage door statelijke actoren.

**Bron:** AIVD – Economische veiligheid en digitale spionage, geraadpleegd september 2026.



# NIS2: wat betekent dit voor jouw maakbedrijf?

Sinds 15 augustus 2026 geldt de Cyberbeveiligingswet in Nederland. Daarmee is NIS2 in Nederlandse wetgeving opgenomen. Valt jouw maakbedrijf onder de wet? Dan moet je aantoonbaar werk maken van het beheersen van cyberrisico's.

## Wanneer val je formeel onder de wet?

Niet ieder maakbedrijf valt automatisch onder de Cyberbeveiligingswet. Vervaardiging is wel één van de aangewezen sectoren. Daarbinnen gaat het onder meer om fabrikanten van computers en elektronica, elektrische apparatuur, machines, motorvoertuigen en andere transportmiddelen.

Ook de omvang van je organisatie telt. Als hoofdregel val je binnen een aangewezen sector onder de wet als je 50 of meer medewerkers (fte) hebt. Heb je minder dan 50 medewerkers, dan kan de wet alsnog gelden wanneer zowel je jaaromzet als je balanstotaal hoger is dan €10 miljoen. Partner- en verbonden ondernemingen kunnen meetellen bij deze beoordeling.

Twijfel je of jouw organisatie onder de wet valt? Gebruik de officiële NIS2-zelfevaluatie van de Rijksinspectie Digitale Infrastructuur.



**Bronnen:** RDI – Cyberbeveiligingswet en sector vervaardiging; NCSC – Cyberbeveiligingswet/NIS2. Geraadpleegd september 2026.

# Wat moet je regelen?

NIS2 vraagt niet om één standaardpakket. Je moet je belangrijkste risico's kennen, passende maatregelen nemen en toetsen of die in de praktijk werken. Voor een maakbedrijf betekent dat onder meer:

### Stap 1

#### **Weet wat kritisch is voor je productie**

Breng in kaart welke systemen, machines, data en digitale koppelingen je nodig hebt om te kunnen produceren. Bepaal ook wat er gebeurt als een systeem een uur, een dag of langer niet beschikbaar is.

### Stap 2

#### **Beperk toegang en kwetsbaarheden**

Houd kritieke systemen actueel, pak bekende kwetsbaarheden tijdig aan en gebruik multifactor-authenticatie (MFA). Geef medewerkers en externe partijen alleen toegang tot wat ze nodig hebben. Besteed extra aandacht aan remote toegang tot machines en scheid IT en OT waar mogelijk van elkaar.

### Stap 3

#### **Zorg dat je kunt doorwerken én herstellen**

Maak betrouwbare back-ups van kritieke systemen en data. Bepaal vooraf wat als eerste moet worden hersteld en test regelmatig of terugzetten ook echt lukt.

### Stap 4

#### **Ken de zwakke schakels in je keten**

Breng in kaart van welke softwareleveranciers, IT-partners, machineleveranciers en onderhoudspartijen je productie afhankelijk is. Maak afspraken over beveiliging, toegang en wat er gebeurt bij een incident.

### Stap 5

#### **Zorg dat je weet wat je moet doen als het misgaat**

Leg vast wie beslist, technisch ingrijpt, klanten informeert en incidenten meldt, en houd dit actueel. Voor significante incidenten geldt een gefaseerde meldplicht: een eerste waarschuwing binnen 24 uur, een vervolgmelding binnen 72 uur en een eindverslag binnen één maand na de melding.

# Ook buiten NIS2 telt je cyberweerbaarheid

Valt jouw organisatie niet rechtstreeks onder de Cyberbeveiligingswet? Ook dan kan NIS2 relevant zijn. Klanten die wél onder de wet vallen, moeten hun ketenrisico's beheersen en kunnen daardoor hogere cybersecurity-eisen stellen aan leveranciers. Sterke cyberweerbaarheid helpt je dus niet alleen om je productie te beschermen. Het kan ook steeds belangrijker worden om een betrouwbare ketenpartner te blijven.

**Bronnen:** NCSC – Cyberbeveiligingswet (toepassingsbereik, zorgplicht en meldplicht); RDI – NIS2-zelfevaluatie. Geraadpleegd september 2026.



## Stap 6

### Houd zicht op wat er in je systemen gebeurt

Continue monitoring helpt om afwijkend gedrag en mogelijke dreigingen vroeg te signaleren, zodat je sneller kunt ingrijpen. Verschillende oplossingen kunnen daarbij helpen:

- EDR (Endpoint Detection & Response): bewaakt laptops, servers en andere endpoints op verdacht gedrag en kan bij een dreiging direct actie ondernemen.
- MDR (Managed Detection & Response): monitoring en respons door externe securityspecialisten die dreigingen analyseren en helpen om snel in te grijpen.
- SIEM (Security Information & Event Management): verzamelt en analyseert informatie uit verschillende systemen om afwijkingen en mogelijke dreigingen zichtbaar te maken.
- SOC (Security Operations Center): een gespecialiseerd team dat beveiligingsmeldingen bewaakt en analyseert en bij een dreiging of incident in actie komt.

Welke vorm bij je bedrijf past, verschilt per organisatie. Belangrijk is dat je dreigingen tijdig signaleert én vooraf weet wie in actie komt.

## Stap 7

### Maak cyber onderdeel van je bedrijfsvoering

Train medewerkers, oefen incidenten en toets regelmatig of je maatregelen nog passen bij je risico's. Nieuwe machines, software, leveranciers, overnames en AI-toepassingen kunnen je risicoprofiel veranderen. Het bestuur heeft hierin een actieve verantwoordelijkheid.

Een goede digitale weerbaarheid verkleint niet alleen de kans op een cyberincident en helpt de impact te beperken. Ook voor een cyberverzekering is dit belangrijk. Verzekeraars stellen eisen aan de beveiliging van je organisatie om dekking te kunnen bieden of behouden. Hoe sterker je digitale weerbaarheid, hoe beter je bovendien in staat bent om je cyberrisico aantoonbaar te beheersen.

# Kan jouw directie deze 10 vragen beantwoorden?

Cyberweerbaarheid is niet alleen een IT-vraagstuk. Deze tien vragen helpen directies van maakbedrijven om snel te zien waar digitale afhankelijkheden, continuïteitsrisico's en bestuurlijke keuzes samenkomen. Kun je niet iedere vraag met zekerheid beantwoorden? Dan weet je waar het volgende gesprek over cyberweerbaarheid moet beginnen.

Welke ontwerpen, productdata of andere intellectuele eigendommen zijn voor een aanvaller het meest waardevol?

Weten we wie we moeten bellen als vannacht de productie stilvalt?

Welke externe partijen hebben op afstand toegang tot onze machines of productieomgeving?

Kunnen we produceren als ons ERP-systeem 72 uur niet beschikbaar is?

Van welke externe leveranciers en digitale diensten zijn we afhankelijk om onze productie draaiende te houden?

Wat kost één dag productiestilstand ons?

Welke vijf digitale systemen zijn essentieel om te kunnen produceren?

Zijn onze IT- en OT-omgevingen voldoende van elkaar gescheiden?

Is ons risicoprofiel veranderd doordat we leveren aan defensie, semicon of andere strategische sectoren?

Hebben we een cyberincident daadwerkelijk geoefend met directie, IT én operations?



# Wat als het toch misgaat?

Goede cyberweerbaarheid verkleint de kans op een incident en helpt je sneller herstellen. Maar niet ieder risico kun je uitsluiten. Dan is de vraag: welke financiële gevolgen kun je zelf dragen en welke wil je verzekeren?

## Wat doet een cyberverzekering?

Een cyberverzekering helpt financiële schade op te vangen én geeft je bij een incident toegang tot specialisten die helpen de schade te beperken en je bedrijfsvoering weer op gang te krijgen.

## Als het misgaat, telt iedere minuut

Een belangrijk voordeel van een cyberverzekering is dat je er bij een incident niet alleen voor staat. Via een speciaal noodnummer krijg je 24/7 toegang tot een Cyber Incident Response Manager. Deze coördineert de aanpak en schakelt afhankelijk van de situatie direct de juiste specialisten in.

Denk aan IT-forensische onderzoekers, juristen, privacy-experts, communicatieadviseurs en schade-experts. Zij werken vanuit hun eigen expertise aan hetzelfde doel: het incident beheersen, de impact beperken en je bedrijfsvoering zo snel mogelijk herstellen.

### Eigen schade

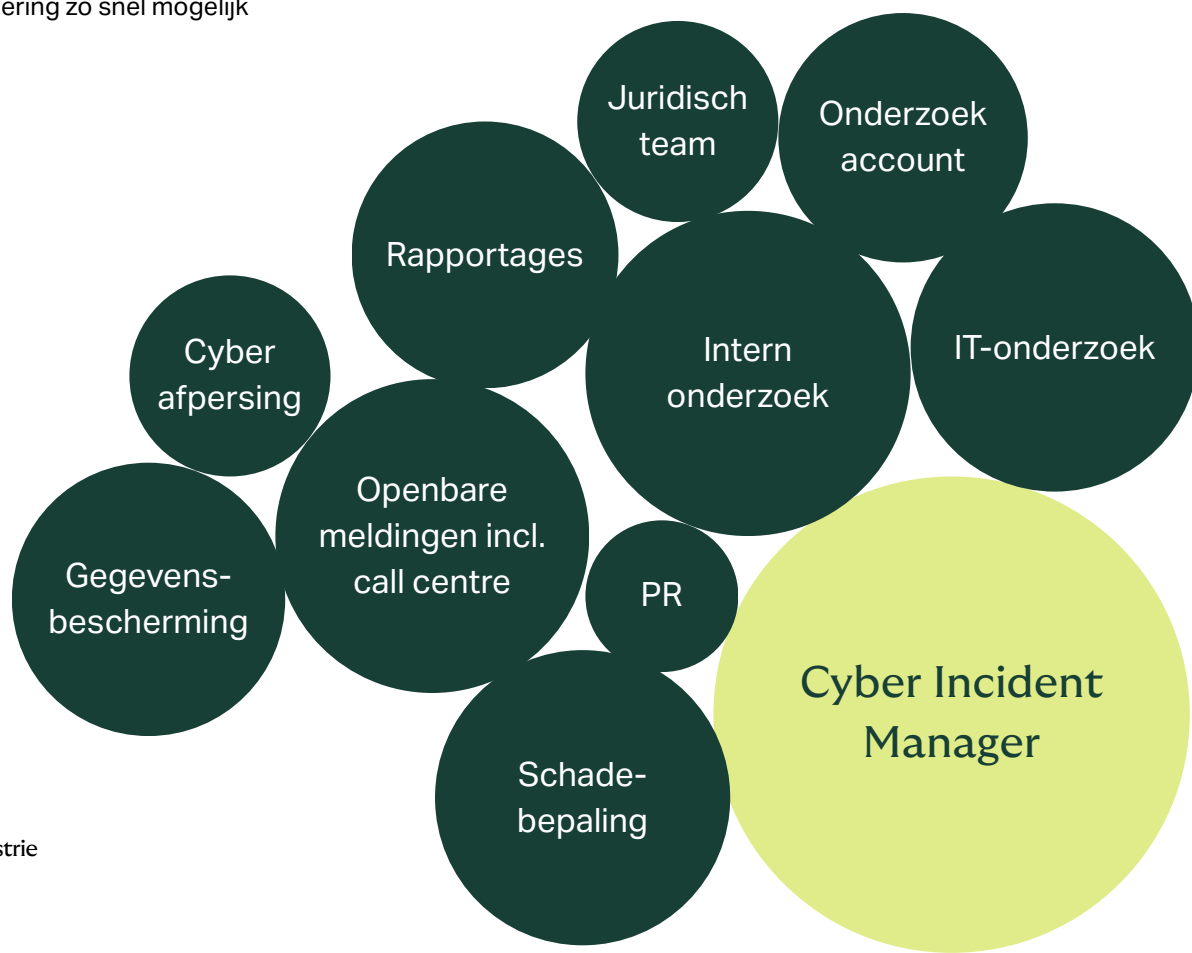
- Bedrijfsschade en omzetverlies
- Herstel van systemen en data
- Cyberafpersing
- Aanvullende herstel- en responskosten

### Incident response

- IT-forensisch onderzoek
- Juridische ondersteuning
- Crisiscommunicatie
- Ondersteuning bij notificatie en privacy-verplichtingen

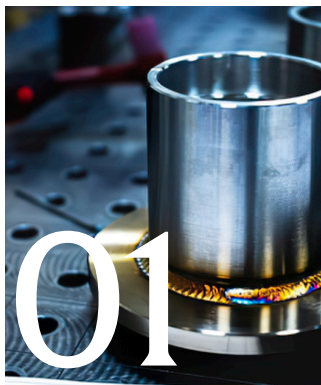
### Aansprakelijkheid

- Aanspraken van derden
- Juridische bijstand
- Privacygerelateerde aansprakelijkheid
- Onderzoek door toezichthouders



# Onze cyberverzekeringen

Geen organisatie is hetzelfde. Omvang, digitale weerbaarheid, internationale activiteiten en de complexiteit van je cyberrisico bepalen welke aanpak past. Daarom biedt Howden verschillende cyberoplossingen, van Cyber+ en Safe+ tot volledig maatwerk.



## Cyber+

Voor bedrijven met een omzet tot €500 mln

Cyber+ combineert brede financiële bescherming met actieve risicomonitoring en 24/7 specialistische ondersteuning als het misgaat. Met slechts vier vragen is het aanvraagproces eenvoudig, krijg je snel inzicht in de mogelijkheden voor jouw organisatie en heb je toegang tot de juiste expertise om de impact van een incident te beperken.



## Safe+

Voor bedrijven met een omzet van €500 mln tot €5 mld

Safe+ is ontwikkeld voor grotere en complexere organisaties. Met slechts zes vragen is het aanvraagproces eenvoudig en krijg je toegang tot brede cyberdekking, waarbij je digitale weerbaarheid wordt meegenomen in de verzekeringsvoorwaarden. Sterke cybersecurity-maatregelen kunnen daarbij worden beloond met ruimere dekking en gunstigere voorwaarden.



## Maatwerk cyberprogramma

Voor bedrijven vanaf €5 mld omzet of met complexe risico's

Voor zeer grote, internationaal actieve of complexe organisaties is een standaardoplossing niet altijd passend. Dan stellen we samen een cyberprogramma op dat aansluit bij je risicoprofiel, internationale activiteiten en verzekeringsbehoeften. Hierbij kijken we o.a. naar:



Passende dekking en programmastructuur



Internationale ondersteuning via het Howden One Network



Geïntegreerde Cyber- en Tech PI-oplossingen waar gewenst



Cybersecurity-ondersteuning door gespecialiseerde experts

## Heb je al een cyberverzekering? Blijf toetsen.

Je cyberrisico verandert mee met je bedrijf. Groei, overnames, nieuwe locaties, internationalisering en veranderingen in je supply chain kunnen invloed hebben op de mogelijke schade. Controleer daarom periodiek of je verzekerd bedrag, eigen risico, voorwaarden, dekkingen en afhankelijkheden van derden nog aansluiten bij je organisatie.



## Hoe cyberweerbaar is jouw organisatie?

Goede bescherming begint met inzicht. Waar ben je kwetsbaar? Wat kan een incident betekenen voor je productie? En welke risico's wil je voorkomen, beperken, zelf dragen of verzekeren? Onze risk consultants brengen het graag samen met je in kaart.

Bezoek [www.howdennederland.nl/cyberverzekering](http://www.howdennederland.nl/cyberverzekering) voor meer informatie of neem contact op met ons een van onze risk consultants.

# Over Howden

Howden is een wereldwijd collectief van ervaren professionals die innovatieve verzekeringsoplossingen ontwikkelen om jouw bedrijfsdoelen te ondersteunen. Als dé risicoadviseur voor ondernemend Nederland helpt Howden jouw organisatie met strategisch risicomanagement, private insurance, verzuim en pensioen.

Onze aanpak richt zich direct op het vergroten van zakelijke kansen en het minimaliseren van risico's, waardoor jij met vertrouwen kunt ondernemen. Door onze diepgaande expertise en toewijding zorgen we ervoor dat je niet alleen voorbereid bent op onzekerheden, maar ook optimaal kunt profiteren van groeimogelijkheden. Zo helpen we jou bij het realiseren van jouw ambities en het waarborgen van de continuïteit van je bedrijf.

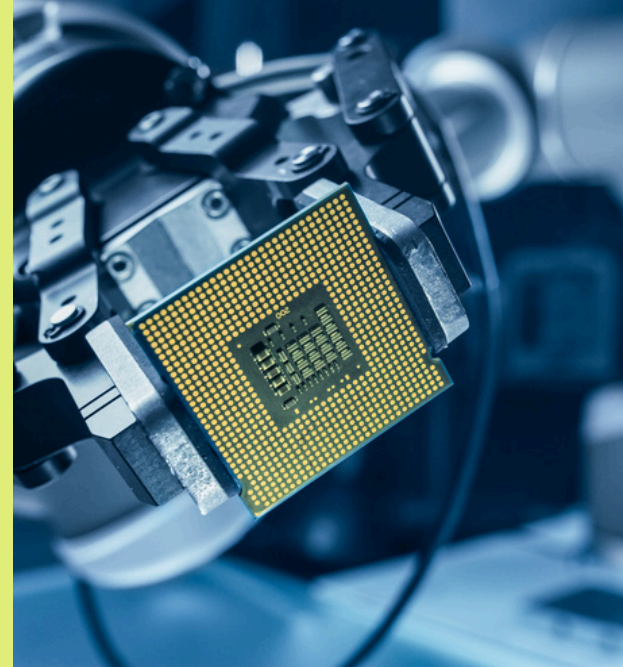
## Persoonlijk en lokaal, met de kracht van een wereldwijd netwerk



# Jouw persoonlijke risicoadviseur in de innovatieve maakindustrie

Bij Howden werken we met een gespecialiseerd sectorteam voor de maakindustrie. Dit team, gevestigd in Eindhoven, richt zich onder andere op de Brainport-regio. Naast jouw persoonlijke risk consultant heb je ook altijd een vast contactpersoon in onze binnendienst. Door gezamenlijk de risico's grondig in kaart te brengen, helpen wij jou inzicht te krijgen in de kwetsbaarheden én kansen om de organisatieveerkracht te vergroten.

Voor meer informatie bezoek  
[www.howdennederland.nl/maak](http://www.howdennederland.nl/maak)



## Interesse in onze dienstverlening?

Neem dan contact op met een van onze accountmanagers. Zij kunnen je verder informeren en een afspraak met je maken.

Howden Eindhoven  
Prof. Dr. Dorgelolaan 14  
5613 AM Eindhoven

T 073 692 46 57  
E [eindhoven@howdennederland.nl](mailto:eindhoven@howdennederland.nl)



**Wesley Stolzenbach**

T +31 6 4063 8750  
E [wesley.stolzenbach@howdennederland.nl](mailto:wesley.stolzenbach@howdennederland.nl)



**Jarno Holleman**

T +31 6 4291 1625  
E [jarno.holleman@howdennederland.nl](mailto:jarno.holleman@howdennederland.nl)



**Gerbert van der Velden**

T +31 6 2458 9754  
E [gerbert.vandervelden@howdennederland.nl](mailto:gerbert.vandervelden@howdennederland.nl)



**Robert Gerrits**

T +31 6 2458 9744  
E [robert.gerrits@howdennederland.nl](mailto:robert.gerrits@howdennederland.nl)



**Michiel van de Moosdijk**

T +31 6 2458 9701  
E [michiel.vandemoosdijk@howdennederland.nl](mailto:michiel.vandemoosdijk@howdennederland.nl)

