



TRENDRAPPORT JUNI 2022

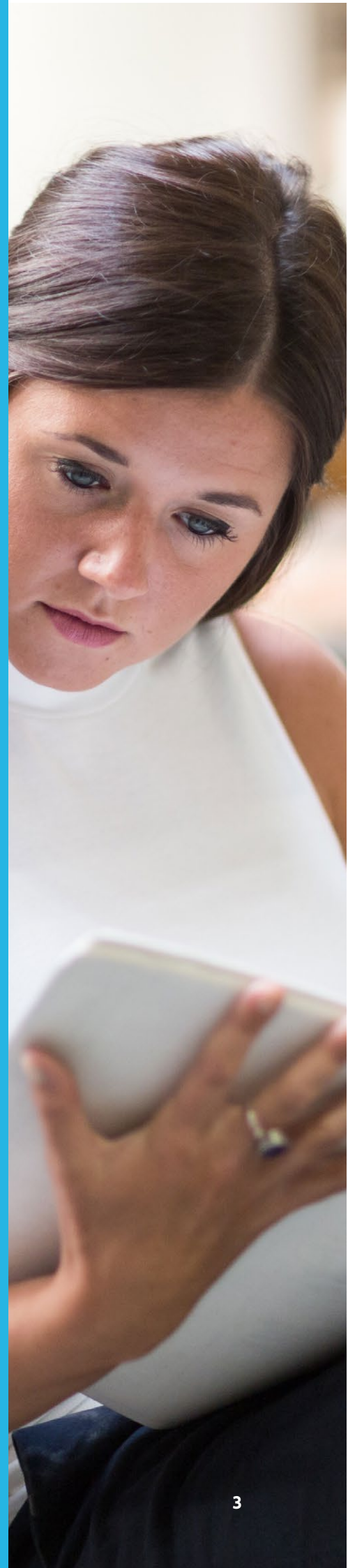
# De status van bedrijfsfraude in de Benelux

51% van de bedrijven had afgelopen 2 jaar  
te maken met fraudepogingen

# Fraude!

## Hoe kan je dat eigenlijk voorkomen?

|                                                 |    |
|-------------------------------------------------|----|
| 1. Inleiding                                    | 5  |
| 2. Verantwoording                               | 6  |
| 3. Resultaten                                   | 8  |
| 3.1 Top 3 meest voorkomende interne fraude      | 9  |
| 3.2 De risico's van thuiswerken                 | 11 |
| 3.3 Factuurfraude koploper van externe fraude   | 14 |
| 3.4 Fraudepogingen detecteren of voorkomen      | 18 |
| 3.5 Fraudeverzekeringen versus cyberverzekering | 21 |
| 4. Conclusie                                    | 23 |





# 1. Inleiding

## Toelichting op het onderzoek

Fraude kent vele verschijningsvormen en fraudeurs zijn creatief, ze leren snel nieuwe methoden en maken steeds vaker gebruik van geavanceerdere technieken. Ze zijn continu op zoek naar nieuwe mogelijkheden en gaan steeds brutaler te werk.

### Bedrijfsleven kwetsbaarder

Onder fraude verstaan we opzettelijke misleidingen om onrechtmatig voordeel te verkrijgen. Vaak financieel voordeel, maar het kan ook gaan om goederen of fraude op de werkvloer ten gunste van de eigen positie. Met het toenemend gebruik van het internet via een verscheidenheid aan devices, wordt steeds meer duidelijk dat organisaties kwetsbaarder zijn voor verschillende vormen van fraude. De dreiging van buiten de organisatie groeit vooral omdat beroepscriminelen zich steeds meer richten op het bedrijfsleven. Vooral digitale fraude is een serieus probleem waar veel ondernemers in toenemende mate last van hebben. Uit het onderzoek blijkt dat 51% van de bedrijven de afgelopen twee jaar te maken heeft gehad met fraudepogingen.

Allianz Trade en Hoffmann Bedrijfsrecherche hebben dit jaar onderzoek uitgevoerd in de Benelux om inzicht te krijgen in de huidige stand van zaken binnen het bedrijfsleven op het gebied van fraude.

Het onderzoek spitst zich toe op verschillende vormen van fraude en in hoeverre bedrijven recent slachtoffer waren van fraude. Het onderzoek betrof ook vragen over de maatregelen die ondernemers nemen om hun weerbaarheid te vergroten.

Kortom, zijn organisaties voldoende beschermd tegen allerlei vormen van interne en externe fraude en wat doen ze om zich hiertegen te beschermen?

Welke conclusies kunnen we hieruit trekken en wat kan het bedrijfsleven hiervan leren?

**Allianz**  | **Allianz Trade**

“51% Van de bedrijven heeft te maken gehad met fraudepogingen in de afgelopen 2 jaar.”



## 2. Verantwoording

Voor dit onderzoek is een vragenlijst uitgezet bij een doelgroep van ruim 900 ondernemers via diverse organisaties en branches in Nederland en België. In totaal vulden 202 ondernemingen de vragenlijst in (132 in Nederland - 69 in de België en Luxemburg), een respons van 22,4 procent.

### Rollen en functies

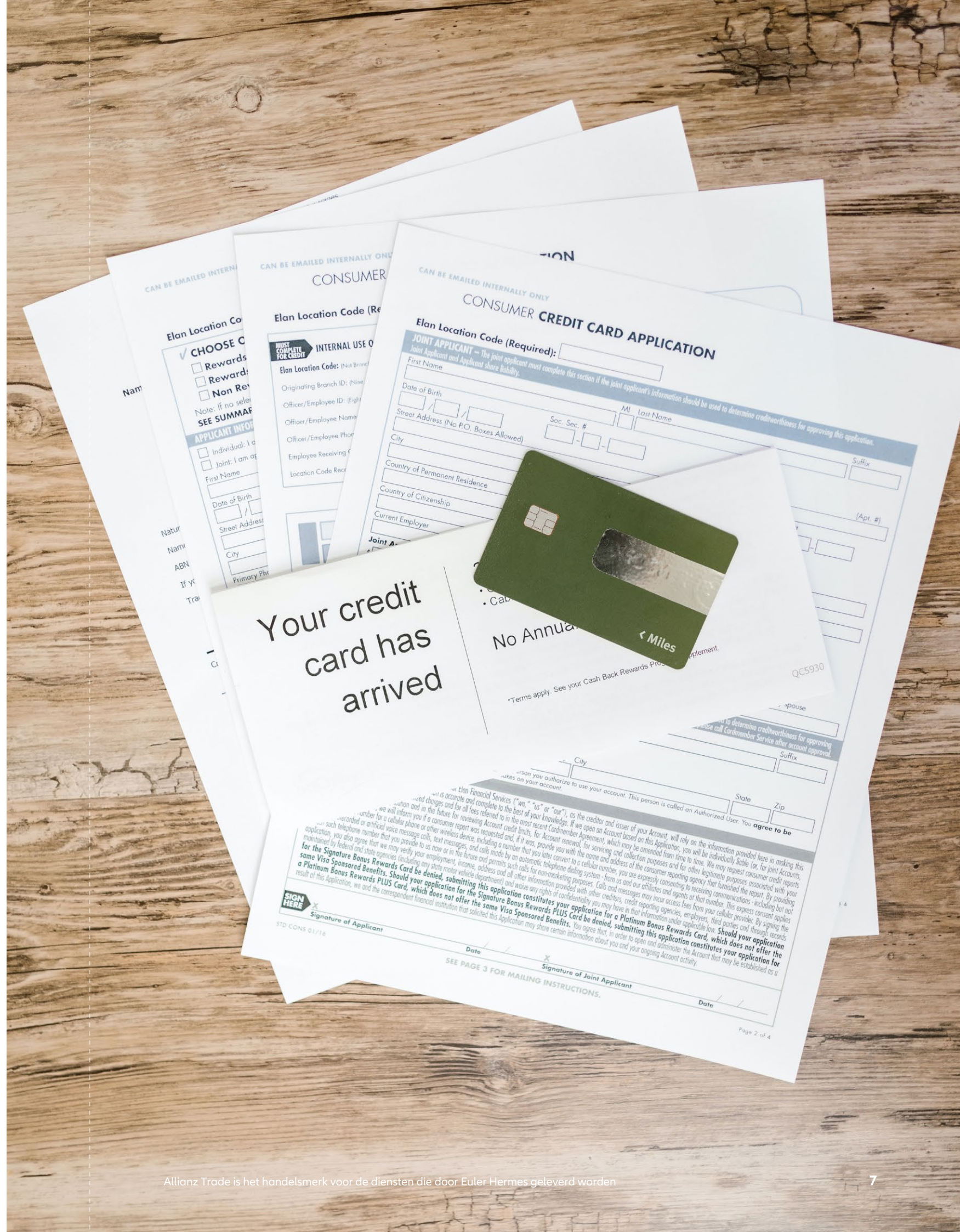
De functietitels van respondenten zijn zeer divers; CEO, CFO's, Risk Managers, Controllers, CTO's en HRM Managers. Ongeveer 62% van de respondenten is algemeen of financieel eindverantwoordelijk. In deze rol zijn zij verantwoordelijk voor het managen van het frauderisico binnen hun organisatie.

### Verdeling sectoren

De sectoren waar de respondenten werkzaam zijn en de omvang van hun organisaties, zijn heel divers. De deelnemende bedrijven vertegenwoordigen een aantal verschillende branches, zoals de bouw en installatie (21%), agri/food (21%), metaal (17%), chemie (5%), transport & logistiek (5%), zakelijke dienstverlening (2%) en overige branches. 46% van de bevroegde personen werkt bij een organisatie met een omzet tussen de €10 en €50 miljoen.

Het onderzoek is uitgevoerd door RVS Marketing in opdracht van Allianz Trade.

's-Hertogenbosch / Antwerpen, juni 2022





# 3. De resultaten

De kans op succes van fraudeurs neemt toe als hun acties sterk lijken op “gangbare” communicatie. Daarin worden fraudeurs steeds beter.

De informatie over ons zakelijke en sociale leven delen we graag en veel online, in het bijzonder via social media. Deze informatie gebruiken criminelen om hun acties goed voor te bereiden. Zo wordt het voor hen makkelijker om ons te misleiden. De oplichtingstechnieken verbeteren van jaar tot jaar en dat is terug te zien in de verschillende vormen waarin fraude en oplichting zich manifesteert.

**Sterke toename fraude en oplichting:**  
**“2 op de 3 respondenten geeft aan dat er MEER fraude en oplichting is gepleegd dan het jaar ervoor.”**

## Dezelfde fraude, nieuwe manieren

Het idee leeft dat criminelen stuk voor stuk slinkse hackers zouden zijn, maar niets is minder waar. Doorgaans is hun aanpak verrassend eenvoudig en betreft het mensen uit de eigen organisatie en gaat het niet altijd om grootschalige financiële fraude. Reden temeer om te allen tijde alert te blijven. Het fraude risico neemt toe; maar liefst 66% van de respondenten geeft aan dat er meer fraude is gepleegd dan het jaar daarvoor.

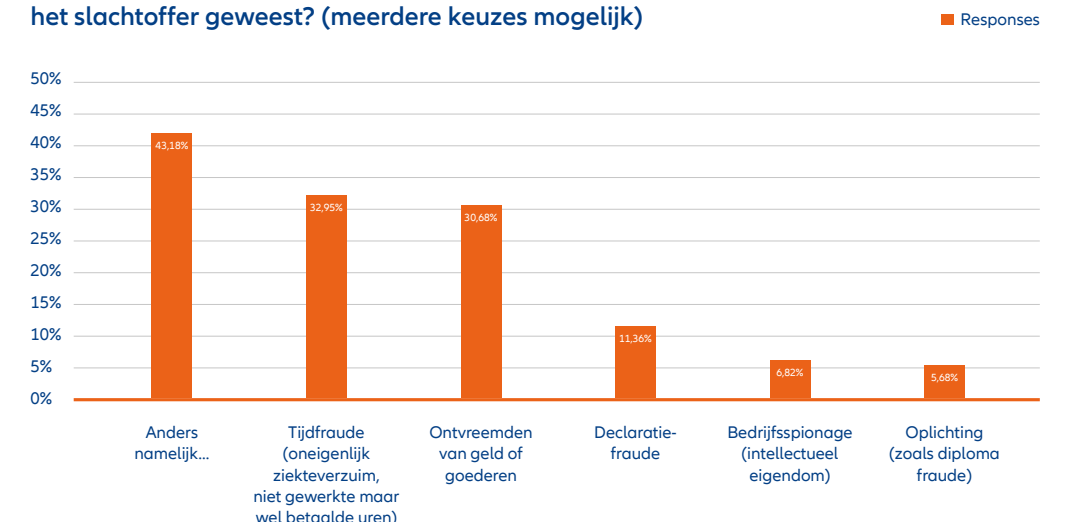
## 3.1 Top 3 meest voorkomende interne fraude

Ruim de helft van de deelnemers aan het onderzoek (51%) heeft het afgelopen jaar te maken gehad met fraude of oplichting.

Van alle interne bedrijfsfraude in het afgelopen jaar is 33% uit tijdfraude. Het is daarmee de meest voorkomende vorm van interne fraude in dit onderzoek. Daarna volgt ‘ontvreemden van geld’ met 31% en de top 3 wordt afgesloten met declaratiefraude (11%).

Tijdfraude is een groeiend probleem. Niet alleen dankzij thuiswerken, maar ook door de verleiding om je makkelijk ziek te melden te melden met corona is een reden. Minder controle betekent simpelweg een groter risico op tijdfraude.

**Van welke soorten interne fraude is jouw bedrijf de laatste 3 jaar het slachtoffer geweest? (meerdere keuzes mogelijk)**



Het ontvreemden van geld of goederen scoort met 31% ook zeer hoog. Medewerkers die geld of goederen van het bedrijf ontvreemden, blijft een probleem met dikwijls zeer hoge financiële impact voor het bedrijf. Deze gevallen komen minder in de pers omdat bedrijven hier uiteraard niet graag mee naar buiten treden.



"95% Van de bedrijven geeft aan dat er een toename is in (vooral) digitale fraude"

### 3.2 De risico's van thuiswerken en digitale fraude

Hoewel 66% van de bedrijven vindt dat thuiswerken het risico op fraude niet heeft vergroot, denkt ruim 1/3 daar dus anders over. Daarnaast geeft 54% van de respondenten aan dat er in hun organisatie geen extra maatregelen worden genomen tegen risico's zoals tijdfraude.

"Meer thuiswerken is voor 54% van de respondenten geen reden voor extra maatregelen."

#### Maatregelen op laag pitje

De grootschalige verschuiving naar thuiswerken van de afgelopen twee jaar (vanwege Covid), noodzaakt logischerwijs tot een update van het risicomanagement, zou je zeggen.

Als er zo veel verandert in de omstandigheden waarin wij ons werk doen, dan ligt het voor de hand dat ook de risico's voor de organisatie veranderen. Met als gevolg dat beheersmaatregelen moeten worden aangepast.

De vraag of dit dan ook gebeurt, was een van de thema's in het onderzoek.

De voornaamste conclusie: over het algemeen is men zich bewust van de 'nieuwe' risico's, maar men is minder ver met het nemen van concrete maatregelen. Ook zijn de investeringen in de beheersing van die risico's niet substantieel toegenomen.

#### Wat doen organisaties dan wel om fraude te bestrijden?

De aanschaf en implementatie van technologie die de organisatie beter beschermt tegen bedreigingen van buitenaf, wordt wel geregeld genoemd. Denk aan een veiliger inlogsysteem of VPN-verbinding. Enkele keren werden trainingen voor bewustwording opgegeven.

#### Digitale fraude

Zoals we al hebben benoemd verschuift fraude en oplichting steeds meer naar online. Ondernemingen zijn in steeds grotere mate afhankelijk van ICT. Deze afhankelijkheid brengt risico's met zich mee en de impact van digitale fraude is dan erg groot. Ook uit het onderzoek komt dit ondubbelzinnig naar voren. Liefst 95% van de respondenten geeft aan dat er een toename is in fraude en dan met name digitale fraude.



## Kenmerken van digitale fraude

- **Per e-mail.** Het verzoek komt vaak per e-mail binnen en niet in persoon.
- **Deepfake-technologie.** Door deepfake-technologie wordt gemanipuleerd audio- en videomateriaal steeds overtuigender. (Voorbeeld uit the wall street journal)
- **Onervaren medewerkers.** Het frauduleuze voorstel is vaak gericht tot iemand die nog niet zo lang binnen de organisatie actief is.
- **Tijdsdruk.** Het verzoek is vaak tijdsgevoelig; het móét bijvoorbeeld vandaag nog worden uitgevoerd.
- **Geheimhouding.** Er mag of kan niet over gecommuniceerd worden, bijvoorbeeld als het gaat om belangrijke zakelijke transacties (zoals een overname, belangrijke betalingen)
- **Voorname afzender.** De vraag komt van een hooggeplaatst persoon of belangrijke partij.
- **Afwijkend van procedure.** De crimineel stuurt vaak aan op een proces buiten de normale procedure (vanwege bijvoorbeeld tijdsdruk).
- **Internationaal.** Vaak is er een internationaal aspect aan verbonden.





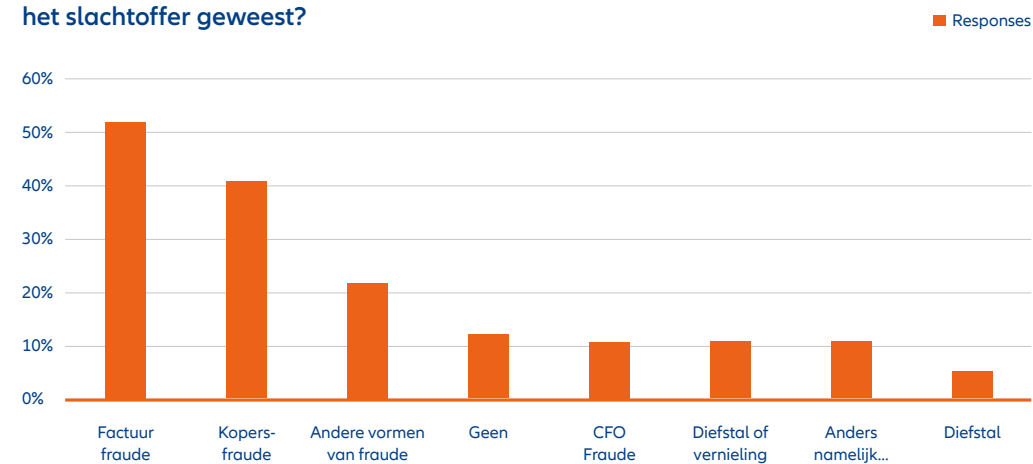
### 3.3 Factuurfraude koploper bij externe fraude

53% van de respondenten gaf aan dat zij de afgelopen 3 jaar slachtoffer zijn geweest van factuurfraude.

Bij factuurfraude wordt de factuur door de (onoplettende) ondernemer betaald naar een vervalste afzender en/of rekeningnummer.

Criminelen misbruiken de vertrouwensrelatie tussen een klant en zijn vaste leverancier door valse facturen in naam van de leverancier te versturen. Dankzij internet zijn tegenwoordig alle gegevens, inclusief logo, online terug te vinden. Dat maakt het voor oplichters een stuk makkelijker.

**Van welke soorten externe fraude is jouw bedrijf de laatste 3 jaar het slachtoffer geweest?**



Als tweede meest voorkomende externe fraude is kopersfraude, ook wel fake buyer fraud genoemd, met maar liefst 41% de runner up. Als derde op de frauderanglijst staat met 23% "overige vormen van identiteitsfraude" naast CEO-fraude die op de vierde plek is geëindigd.

#### Grote impact, maar ook 'gevoelig'

CEO-fraude lijkt dan ook minder voor de komen, maar dat kan ook te maken hebben met de publiciteitsgevoeligheid. Bedrijven die slachtoffer worden van deze vorm van fraude, stappen niet zo snel naar de media. Maar toch komt CEO fraude steeds vaker voor. En je ziet het ook steeds meer in de media verschijnen. Dat slimme criminelen zo de jackpot binnen kunnen halen werd duidelijk na een succesvolle scam bij bioscoopketen Pathé (totale schade was 19 miljoen euro) en staalbedrijf Jewo metaal (totale schade was 11 miljoen euro).



### Wat is CEO Fraude?

CEO fraude is een geraffineerde manier van oplichting gericht op bedrijven en grote organisaties. Oplichters doen zich voor als de CEO of CFO, de oprichter of een andere hooggeplaatste manager en proberen op deze manier geld los te peuteren. In de meeste gevallen wordt er contact opgenomen via e-mail met een bericht om dringend geld over te maken. Uiteraard komt dit bericht niet van de echte CEO, maar wordt er misbruik gemaakt van de machtsafstand ten opzichte van de gecontacteerde medewerker. Deze hebben vaak een grote impact, omdat criminelen hierbij grote sommen geld wegsluizen. Bijvoorbeeld als het gaat om belangrijke zakelijke transacties (zoals een overname, belangrijke betalingen).

#### Hoe groot was jouw financiële en materiële schade?

Op de vraag of men daadwerkelijk slachtoffer is geworden van een vorm van fraude, antwoordde net iets meer dan de helft met ja. In totaal 51%, al betrof dit niet altijd financiële schade. Van degenen die wel financiële schade opliepen, ging het in 48% van de gevallen om schade tot 50.000 euro. 10% had een schadepost tussen de 200.000 en 500.000 euro. En 1% zelfs meer dan 5 miljoen.





## Tips tegen identiteits-, factuur- of CEO-fraude?

### 1. Maak fraude bespreekbaar.

Het bewust maken van jouw personeel is een van de belangrijkste maatregelen. Door fraude intern bespreekbaar te maken trappen medewerkers minder snel in valse e-mails of andere vermommingen.

### 2. Creëer een open bedrijfscultuur.

CEO-fraude kent het meeste succes binnen sterk hiërarchische ondernemingen. Het moet voor medewerkers mogelijk zijn om aan hun leidinggevende vragen te stellen en om de bevestiging van een afwijkend betalingsverzoek te vragen. Hoe korter de lijntjes tussen medewerker en leidinggevenden hoe minder de kans op CEO-fraude.

### 3. Bouw checkmomenten in.

Bouw bij de werkzaamheden en processen meer checkmomenten in. Veel ellende is te voorkomen met een gezonde portie argwaan. Check consequent details, zoals het adres en de namen van tekenbevoegden. Verifieer bij twijfel gegevens telefonisch bij je vertrouwde contactpersonen.

### 4. Hou je aan het vierogenprincipe!

Leg afspraken vast voor het overboeken van grotere bedragen met hulp van autorisatieschema's en het vierogenprincipe.

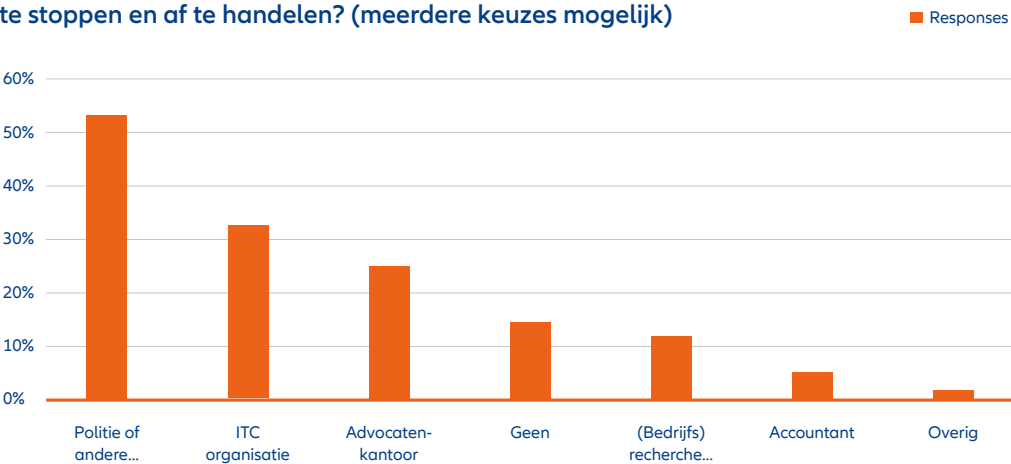


### 3.4 Fraudepogingen detecteren of voorkomen

Op de vraag “In hoeveel gevallen ben je erin geslaagd deze fraudepogingen binnen je eigen organisatie, zonder hulp van externen, te stoppen en af te handelen”, antwoordde 56% van de respondenten dat zij alle gevallen zelf hebben kunnen oplossen.

Toch zie je dat er steeds meer hulp wordt gevraagd aan externe partijen. Onder de overige 45% procent van de ondervraagden, schakelden de meeste bedrijven hulp in van politie of andere overheidsinstellingen, ICT-organisaties, advocatenkantoor of bedrijfsrecherche.

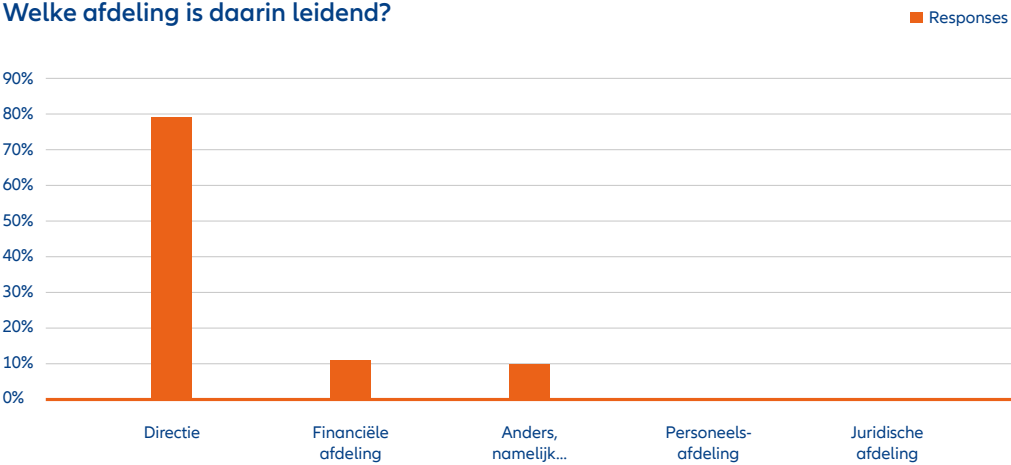
Welke externe partners heb je ingeschakeld om de fraudepogingen te stoppen en af te handelen? (meerdere keuzes mogelijk)



Preventie door wie?

Ondernemers vinden dat de verantwoordelijkheid voor de veiligheid van de digitale omgeving van het bedrijf voornamelijk bij de directie ligt (79%) en 11% vindt dat dit bij de financiële afdeling thuisheert. De HR-afdeling en juridische zaken zijn duidelijk niet leidend hierin. Enkele respondenten vinden dat er verschillende afdelingen verantwoordelijk moeten zijn.

Welke afdeling is daarin leidend?



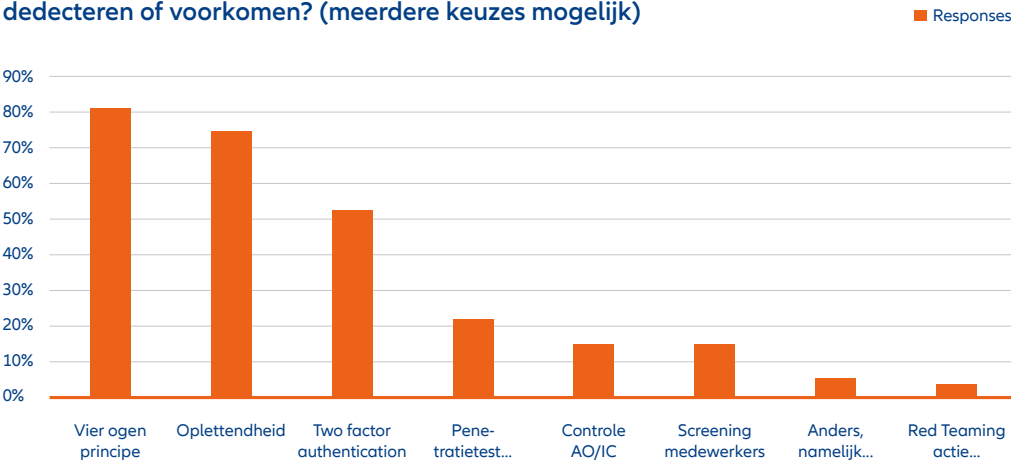
Hoe voorkom je fraude en oplichting?

Niemand wil fraude en iedereen wil het voorkomen. De feiten zijn evenwel dat fraude ook voorkomt bij ondernemingen die zich daarvan eerder geen voorstelling konden maken. Een belangrijke vraag is dan ook, welke maatregelen nemen zij?

Bedrijven passen vaker een of meerdere maatregelen toe om fraude te voorkomen. 81% van de respondenten gebruikt het ‘vier ogen principe’. Dus men laat altijd twee mensen van het

management een betaling fiatteren. 76% van de ondernemingen leunt vooral op de bewustwording en oplettendheid van eigen medewerkers. 53% kiest voor een twee factor authenticatie en 20% voert een penetratietest uit. Een penetratietest (pentest) wordt vaak gebruikt om te laten zien of je organisatie voldoende weerbaar is tegen digitale aanvallen. Een maatregel die minder vaak wordt genomen, is de screening van eigen medewerkers (16%) en ook de controle van AO/IC (16%).

Wat werd hoofdzakelijk gebruikt om deze fraudepogingen te dedecteren of voorkomen? (meerdere keuzes mogelijk)





Risicoanalyse en noodplan

37% van de ondervraagde bedrijven geeft aan ooit een fraude-analyse te hebben uitgevoerd door een verzekeraar, consultant of accountant. In de vorm van een op fraude gerichte risicoanalyse kunnen de risicovolle processen, systemen en functies in kaart worden gebracht. Bedrijven geven aan dat dit grotendeels is gefocust op digitale fraude en op de financiële administratie.

En 67% van de ondervraagden gaf aan geen noodplan achter de hand te hebben. Ondanks een reeks aan maatregelen zijn bedrijven maar gemiddeld tevreden over hun bescherming. Gemiddeld geven zij zichzelf een 7,2 voor fraudebescherming.

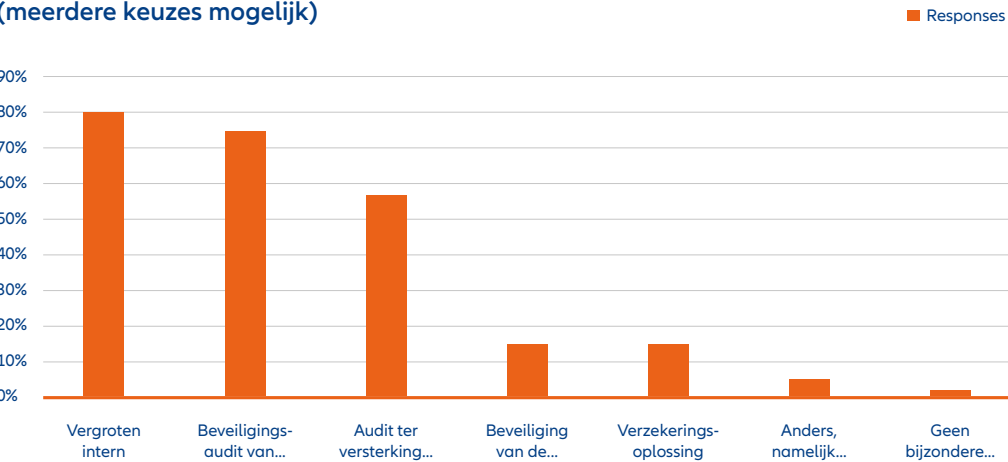
“Bedrijven geven zichzelf een 7,2 gemiddeld voor fraudebescherming.”

Investerings voor de toekomst

Een goede bescherming tegen alle mogelijke gevaren van fraude en oplichting is dus geen overbodig luxe. Dit vertaalt zich ook in het voornemen om hierin meer te investeren (36%). 25% laat de huidige investeringen zoals het nu is en 24% procent laat het nog in het midden.

Daarnaast geven de respondenten aan vooral te willen investeren in het vergroten van het interne bewustzijn of ze willen een beveiligingsaudit uitvoeren. Ook een audit ter versterking van de interne administratieve procedures werd vaak genoemd. Een andere maatregel die terugkomt, is het afdekken van het risico door het afsluiten van een fraudeverzekering.

Waar in wordt er geïnvesteerd in de komende 3 jaar? (meerdere keuzes mogelijk)



3.5 Fraudeverzekeringen versus cyberverzekering

Aan de respondenten is gevraagd of zij een cyber-verzekering hebben afgesloten. 29% gaf aan een cyberverzekering te hebben en 20% is van plan om een cyberverzekering af te sluiten.

Een cyberverzekering is niet hetzelfde als een fraudeverzekering. De fraude-verzekering dekt de financiële gevolgen van fraude door zowel medewerkers als derden. Het is opvallend dat 34% niet bekend is met een fraudeverzekering. 24% heeft al een fraudeverzekering en 11% is van plan om een fraude-verzekering af te sluiten.

Dat de fraude- en cyberverzekering nog weleens verward worden blijkt uit de 46% van de respondenten die in de veronderstelling zijn dat een cyberverzekering voldoende beschermt tegen digitale fraude. Dit is niet het geval. De cyberverzekering beschermt tegen bedrijfsschade door een cyberaanval en tegen aansprakelijkheid voor schade aan derden.

Hierbij kun je denken aan inbreuk op hun privacy of geheimhouding, de kosten van gestolen data, omzetverlies (doordat het bedrijf een bepaalde periode niet operationeel is), cyber-afersing en kosten van het herstel van programmatuur of data.

Als sluitstuk voor hun risicopreventie kunnen bedrijven zich ook verzekeren voor schadelijke gevolgen van fraude. Deze kunnen zich voordoen wanneer de preventieve maatregelen onvoldoende bleken te zijn. Veel bedrijven zijn niet op de hoogte van het bestaan van een dergelijke verzekering. Deze is van belang omdat de cyber-verzekering, kredietverzekering en bedrijfsaansprakelijkheidsverzekering dit financieel verlies door fraude niet dekt.

“46% denkt dat een cyberverzekering voldoende beschermt tegen digitale fraude. Dit is niet het geval.”

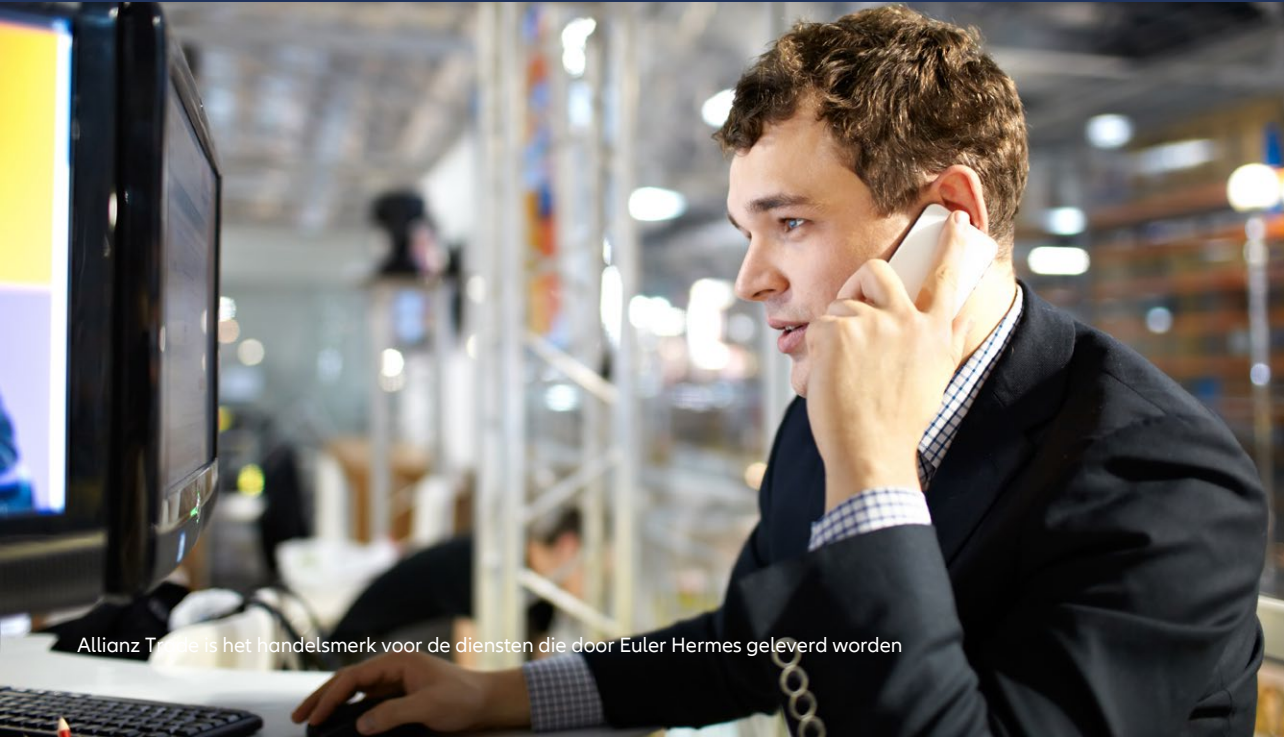


In onderstaande tabel geven we de mogelijke dekkingen van fraude- en cyberverzekeringen weer. Dit overzicht dient om globaal het verschil tussen beide soort verzekeringen te laten zien. Voorwaarden verschillen per verzekeraar. Aan dit overzicht zijn dan ook geen rechten te ontleen, controleer altijd de voorwaarden van de verzekering.

| Fraudeverzekering                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Cyberverzekering                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• (Identiteits)fraude, oplichting, valsheid in geschrifte, diefstal door interne medewerkers.</li><li>• (Identiteits)fraude, oplichting, valsheid in geschrifte, diefstal door derden.<br/><i>Voorbeelden: CEO-fraude, Social Engineering, Deepfake/ Deepvoice, factuurfraude, Fake buyer Fraude, het omleiden van betalingsstomen. Maar ook het stelen van wachtwoorden of omleiden naar andere websites in geval er fraude is/wordt gepleegd.</i></li><li>• Kosten (in geval van fraude): reparatie/schoonmaken van de IT-systemen, telefoonhacking, bereddingskosten, de herstelkosten van reputatieschade, juridische kosten, contractuele boetes en een voorlopige uitkering.</li></ul> | <ul style="list-style-type: none"><li>• Het kapot maken/platleggen van IT-systemen.</li><li>• Reparatie/herstelkosten van de systemen.</li><li>• Bedrijfsschade door een cyberincident (meestal gemaximeerd tot 180 dagen).</li><li>• Schade voor aansprakelijkheid van het stelen van data (inbreuk op privacy/ geheimhouding), kosten intern onderzoek.</li><li>• Schadevergoeding door uitbetalen van ransom/digitale afpersing.</li><li>• Cyber diefstal (meestal gemaximeerd tot bijvoorbeeld 50.000 EUR).</li><li>• Ondersteuning door IT specialisten in geval van een hack en juridische/forensische ondersteuning.</li></ul> |

## Ben je met een cyberverzekering voldoende beschermd?

Je hebt in principe twee aparte verzekeringen nodig om het volledige risico af te dekken tegen diverse vormen van fraude en de daarbij behorende risico's. Door een goede afstemming van deze verzekeringen, weet je zeker dat de financiële schade gedekt is.



Allianz Trade is het handelsmerk voor de diensten die door Euler Hermes geleverd worden

# Conclusie

51% van de respondenten heeft in het afgelopen jaar te maken gehad met een vorm van fraude of oplichting.

66% geeft aan dat dit meer is dan voorgaande jaren.

95% van de bedrijven ziet een toename, met name bij digitale fraude.

Een feit is dan ook dat fraude en oplichting toeneemt.

### Koplopers: tijdfraude en factuurfraude

In de categorie interne fraude komt tijdfraude het meeste voor, gevolgd door ontvreemden van geld en declaratiefraude. Bij externe fraude is factuurfraude de koploper, naast kopersfraude en verschillende vormen van identiteitsfraude. CEO-fraude komt relatief gezien weinig voor, maar levert gemiddeld wel meer schade op.

### Er valt nog veel te winnen met preventie

Op het gebied van preventieve maatregelen valt er nog veel te winnen. Een goede bescherming tegen alle mogelijke gevaren van fraude is geen overbodige luxe voor een bedrijf, zo blijkt. Bedrijven schenken veel aandacht aan de interne bewustwording maar vertrouwen hierbij hun medewerkers volkomen. Niet alleen wat thuiswerken betreft maar ook als het gaat in welke mate medewerkers elkaar onderling in de gaten houden.

Verder blijkt uit onderzoek dat 67% geen noodplan achter de hand heeft.

Bedrijven willen meer investeren in preventieve maatregelen. Maar een grote groep is nog in dubio en weet nog niet wat de plannen zijn op dit gebied.

### Onbekend met verzekeringen

Cyberverzekeringen en fraudeverzekeringen zijn nuttige aanvullingen maar te weinig bedrijven hebben hier voldoende kennis over en zijn niet bekend met deze verzekeringen en de verschillen. Laat staan dat zij weten wat wel of niet onder een polis valt. Beide verzekeringen worden wel beschouwd als een zeer nuttige aanvulling op de fraudepreventieplannen.



Wilt u meer weten over onze oplossingen van kredietverzekering, garantie of fraudeverzekering?  
Neem contact op met ons team. Onze experts helpen u graag.

Bel het nummer **+32 (0)2 790 24 15** of stuur een mail naar **[contact.belux@allianz-trade.com](mailto:contact.belux@allianz-trade.com)**

Ontdek onze website: **[www.allianz-trade.be](http://www.allianz-trade.be)**