Allianz Trade

TRENDRAPPORT 2024

Jaarlijks fraudeonderzoek in Nederland en België

Hoeveel bedrijven en organisaties waren slachtoffer van fraude?

Welke fraude komt het meeste voor?

Welke maatregelen nemen bedrijven?

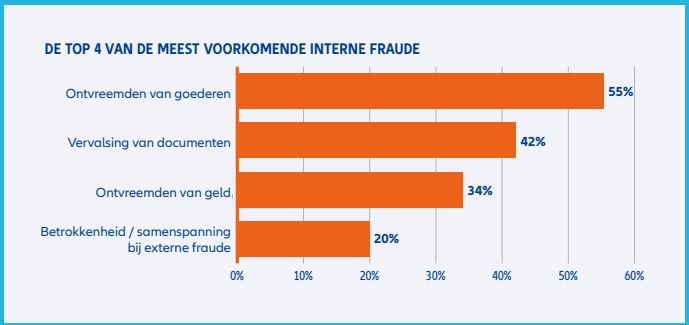
Hoe groot zijn de schades?

Wie zijn de typische fraudeurs?

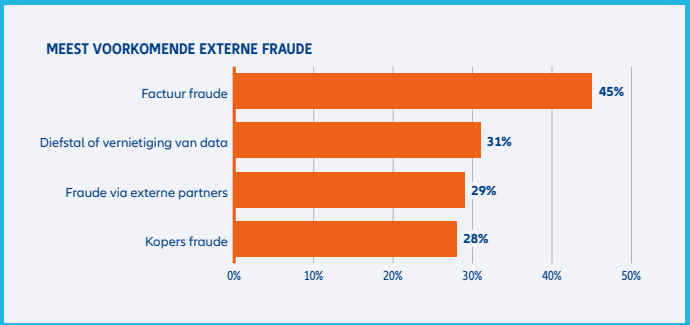
Wat is het effect van AI op fraude?

Resultaten in vogelvlucht

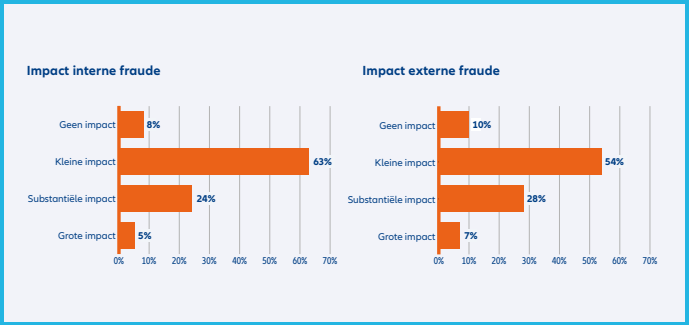
De top 4 van de meest voorkomende interne fraude



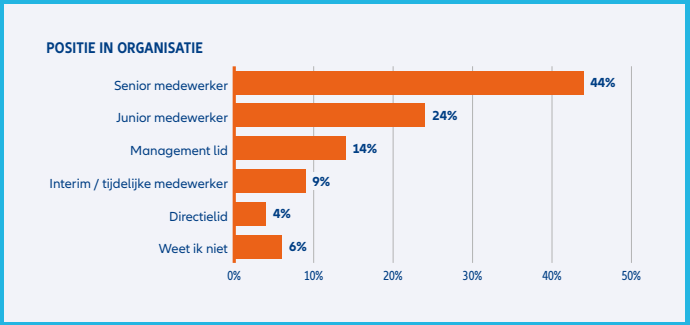
Meest voorkomende externe fraude



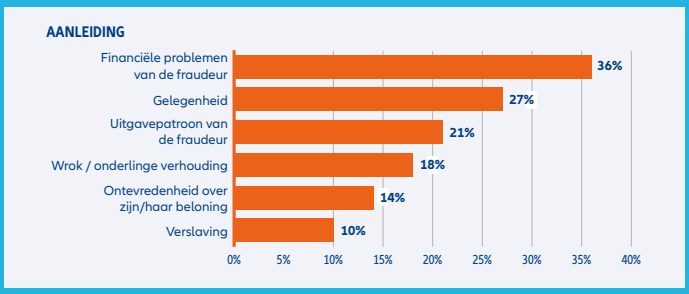
Impact fraude



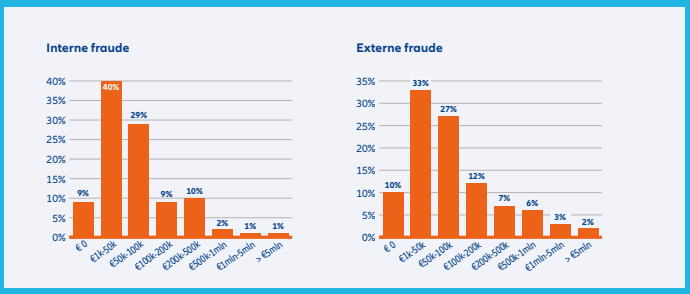
Positie in organisatie



Aanleiding



Geleden schade



1. Inleiding

Toelichting op het onderzoek

Allianz Trade is expert op het gebied van fraude. In navolging van onze fraudeonderzoeken in andere landen voeren we sinds 2022 ook jaarlijks een fraude-onderzoek uit in Nederland en België. Dit is het derde rapport op rij. Het jaarlijks onderzoek toont de actuele stand van zaken op fraudegebied. Het onderzoek spitst zich toe op verschillende vormen van fraude, de schade die bedrijven lijden en de maatregelen die worden genomen. Alles bij elkaar geeft dat een beeld van de weerbaarheid en de kwetsbaarheid van het bedrijfsleven in Nederland en België. Omdat het onderzoek jaarlijks plaatsvindt is het mogelijk actuele fraude-ontwikkelingen te registreren. Aanvullend beoogt het onderzoek ook inzicht te geven in de behoefte van bedrijven en organisaties om zich te beschermen tegen fraude.

2. Verantwoording

In opdracht van Allianz Trade is het onderzoek in het voorjaar van 2024 uitgevoerd door MetrixLab. In totaal werkten 350 bedrijven/organisaties mee aan dit onderzoek (200 in Nederland, 150 in België). 40% betreft B2B-bedrijven, 40% B2C en 20% overheid & non-profit. Alle bedrijven/organisaties hebben een jaaromzet van minstens €10 miljoen en hebben minimaal 50 medewerkers in dienst. Voor het onderzoek hebben de deelnemende organisaties een online-vragenlijst beantwoord.

De rollen en functies van de respondenten zijn zeer divers; van CEO's, CFO's tot controllers en HR-managers. Allemaal zijn ze bij hun organisatie volledig of gedeeltelijk verantwoordelijk voor riskmanagement en het afdekken ervan. De deelnemende organisaties vertegenwoordigen een breed scala aan branches: van transport tot retail, van metaal tot textielindustrie.

Allianz Trade
's-Hertogenbosch / Brussel, juni 2024

3. De resultaten

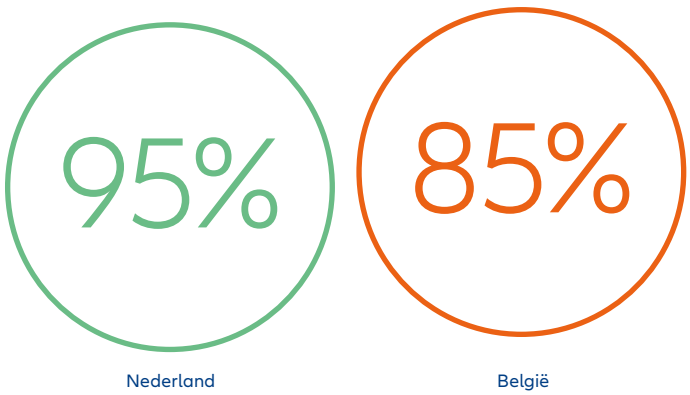
Afname van fraude(pogingen) strooit zand in de ogen

Het algemene beeld dat in het onderzoek van 2024 nadrukkelijk naar voren komt is dat bedrijven en organisaties in toenemende mate vooral technische maatregelen nemen om fraude te voorkomen. Het resultaat hiervan is dat het aantal gevallen van waargenomen fraude(pogingen) met 10% is gedaald in de periode 2023-2024. Ook zien we dat bedrijven en organisaties zich hierdoor in toenemende mate veilig wanen. Dat is schijnveiligheid want nog altijd had 69% van de deelnemende organisaties in de onderzoeksperiode te maken met interne of externe fraude(pogingen). Hierbij zijn de veel voorkomende phishing-mails niet meegeteld. Het idee dat met enkele technische maatregelen het fraudeprobleem afdoende is opgelost is onterecht.

“Bij ons zit het wel goed”

In 2023 vond 85% van de bedrijven en organisaties de eigen bescherming (ruim) voldoende. In 2024 is dit opgelopen naar 91%. Nederlandse organisaties zijn nog tevredener dan Belgische: 95% vs 85%. Er lijkt hier sprake van een vals gevoel van veiligheid. Ruim tweederde van de bedrijven en organisaties had in de onderzoeksperiode te maken met fraude(pogingen).

Tevredenheid Nederland vs België



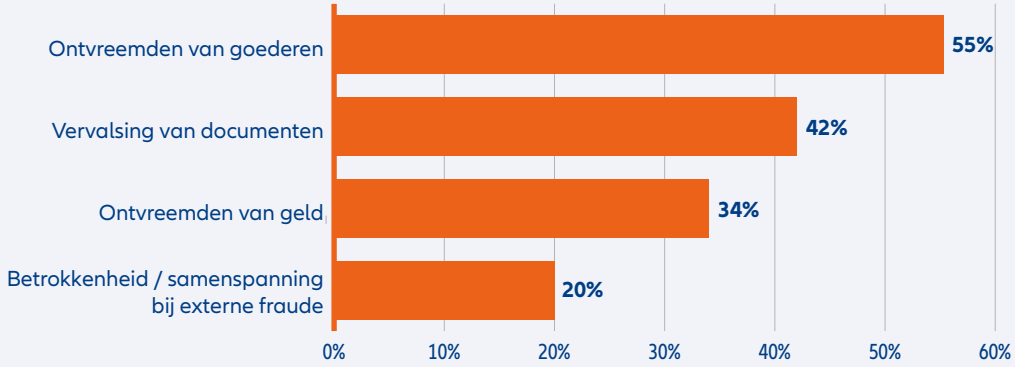
Wat verstaan we onder (interne en externe) fraude?

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. Het toenemend gebruik van het internet via een verscheidenheid aan devices, maakt organisaties steeds kwetsbaarder voor verschillende vormen van fraude. We onderscheiden interne fraude en externe fraude. Interne fraude (door eigen medewerkers) komt nog altijd het meest voor, al wint externe fraude snel terrein omdat beroepscriminelen zich steeds meer richten op bedrijven en organisaties. Vooral digitale fraude is daarbij sterk in opkomst. Organisaties vrezen vooral de opkomst nieuwe technologieën op het gebied van digitale fraudes (zoals deepvoice/deepfake/ nep e-mails). Vooral Artificial Intelligence biedt fraudeurs een zee aan nieuwe mogelijkheden.

3.1. Interne fraude

De daling van het aantal gevallen van fraude (pogingen) gaat niet op voor interne fraude. Die bleef op hetzelfde niveau. Nog altijd wordt de meeste fraude gepleegd door eigen werknemers. 56% van de bedrijven en organisaties had te maken met interne fraude(pogingen).

DE TOP 4 VAN DE MEEST VOORKOMENDE INTERNE FRAUDE

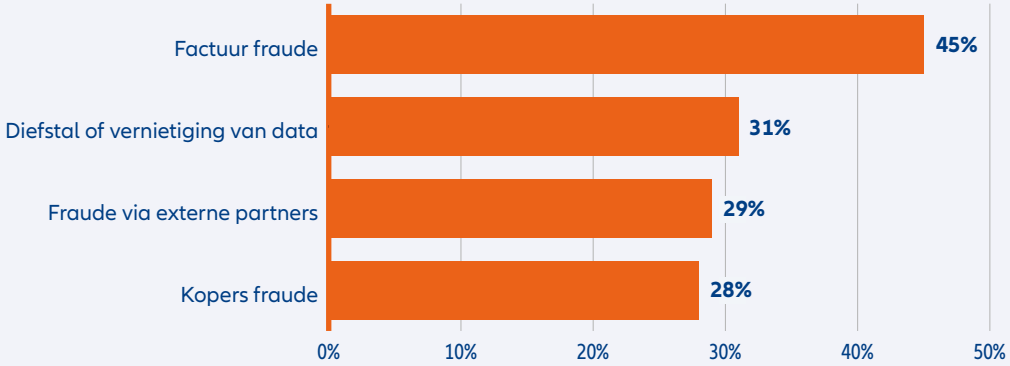


Uit het onderzoek blijkt dat ontvreemden van goederen in België duidelijk meer voorkomt dan in Nederland: 63% vs 49%. In Nederland komt ontvreemden van geld meer voor: 36% vs 30%.

3.2. Externe fraude

Bij externe fraude staat ‘factuurfraude’ nog steeds bovenaan. In Nederland komt het nog meer voor dan in België: 48% vs 40%. In België valt het forse aandeel van ‘kopersfraude’ op: 43% vs 18%.

MEEST VOORKOMENDE EXTERNE FRAUDE



Kopersfraude
Bij kopersfraude (fake buyer fraude) doet een oplichter zich voor als een (bestaande) klant. De nep-koper bestelt goederen en laat deze leveren op een ander adres (niet het echte adres van de klant). De fraudeur kan de goederen ook vóór levering onder valse voorwendselen onderscheppen (bijvoorbeeld via de transporteur).

Tips om interne en externe fraude te voorkomen

1: Maak fraude bespreekbaar.
Het bewust maken van 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 medeweker en leidinggevenden hoe minder de kans op CEO-fraude.

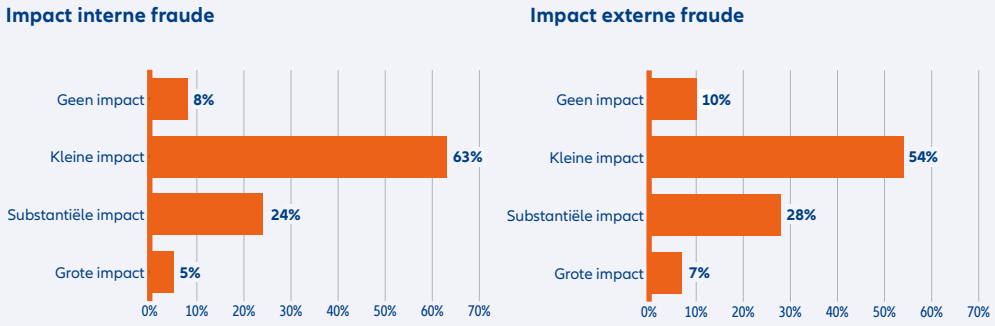
3: Bouw checkmomenten in.
Bouw bij de werkzaamheden en processen meer checkmomenten in. Veel ellende is te voorkomen met een gezonde portie argwaan. Check consequent details, zoals het adres en de namen van contactpersonen/tekenbevoegden. Verifieer bij twijfel gegevens telefonisch bij je vertrouwde contactpersonen.

4. Hanteer het vierogenprincipe!
Leg afspraken vast voor het overboeken van grotere bedragen met hulp van authorisatieschema's en het vierogenprincipe.

3.3. Impact

In de meeste gevallen heeft fraude slechts een kleine impact op organisaties. Dat neemt niet weg dat fraude bij één derde van de gevallen 'substantiële tot grote impact' heeft. Wat opvalt is dat in België de impact van met name interne fraude groter is dan in Nederland.

30% van fraude heeft aanzienlijke impact



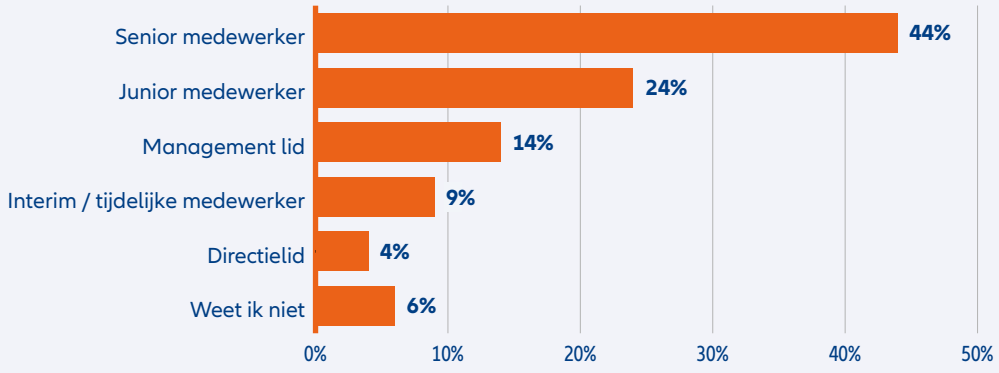
3.4. Profiel interne fraudeur: vooral mannen!

Nog meer dan in het vorige onderzoek geven organisaties en bedrijven aan dat interne fraude gepleegd wordt door mannen (2024: 75%, 2023 64%). Wie is die interne fraudeur? In dit onderzoek is hier nader op ingezoomd. Vaak zijn het mannen die minder dan vijf jaar in dienst zijn. En dan vooral in de leeftijdscategorie van 26 tot 45 jaar (74%). Het gaat daarbij vaak om kleinere schadeposten (in dit onderzoek is €15.000 schade als ondergrens aangehouden).

Nemen we niet het aantal fraudes als uitgangspunt maar de omvang van de schade, dan komen nadrukkelijk de seniors die al langer in dienst zijn in beeld. De oudere, hoger opgeleide fraudeur met vaak leidinggevende taken, kent de bedrijfssystemen en mechanismen door en door. Omdat ze vaak lang in dienst zijn genieten ze bij collega's en superieuren groot vertrouwen. Dat verschaft hen allerlei vrijheden, waaronder toegang tot vertrouwelijke systemen en informatie.

Veel fraude door directie en management
Bijna 20% van (grote) schades door interne fraude wordt veroorzaakt door een lid van directie of management.

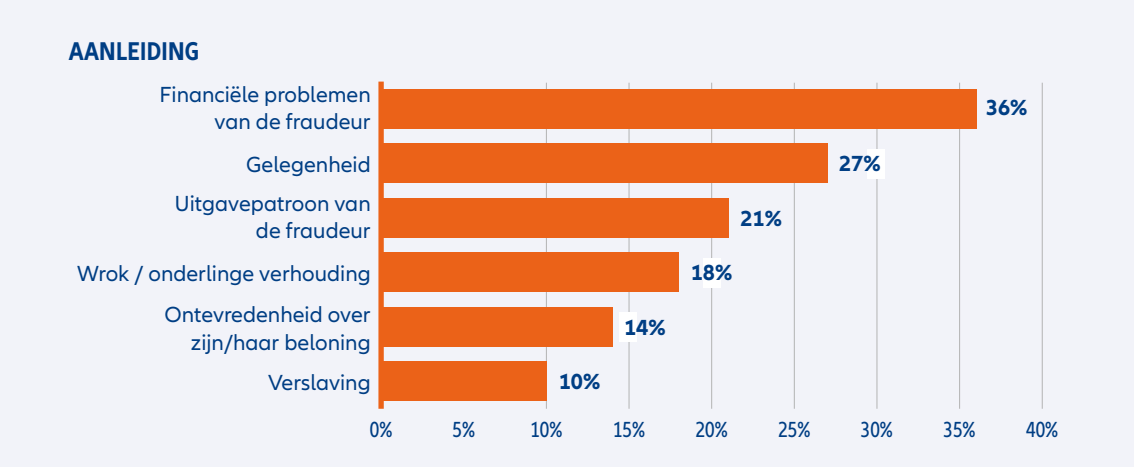
POSITIE IN ORGANISATIE



Vervolg profiel interne fraudeur

Volgens criminoloog Donald Cressey zijn er drie belangrijke voorwaarden die de kans op interne fraude vergroten: gelegenheid, druk en rationalisatie ('goedpraten').

- **Gelegenheid**
  De kans om fraude te plegen zonder betrapt te worden. Dit kan te maken hebben met zwakke interne controlemechanismen, gebrek aan toezicht of eenvoudige toegang tot geld of activa van het bedrijf.
- **Druk (of motivatie)**
  Denk aan financiële problemen vanwege schulden, gokverslaving of de wens om zich bepaalde luxe te veroorloven.
- **Rationalisatie**
  Interne fraudeurs praten hun daad goed. Ze zien diefstal als 'tijdelijk lenen' of 'het bedrijf is rijk genoeg en merkt er niks van'.



Op welke afdelingen wordt het meest gefraudeerd?

Fraudeurs zijn op elke afdeling te vinden. Het hoogst scoort 'Operations' met 27%, daarna Finance met 24%, vervolgens Verkoop 21% en Inkoop 19%. De verschillen zijn beperkt. In het vorige onderzoek stond Finance duidelijk bovenaan.

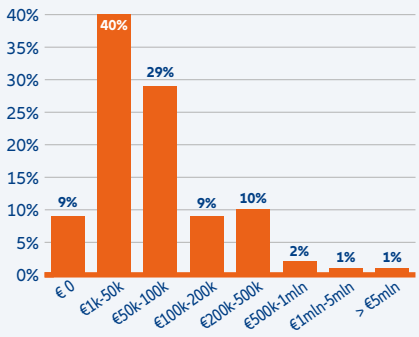
Het is niet zo dat senior medewerkers vaker 'gelegenheid' als aanleiding zien om fraude te plegen. Wel zien we dat senior medewerkers 'wrok' vaker als een aanleiding zien dan de junior medewerkers.

3.5. 16% van fraudeschades hoger dan €200.000

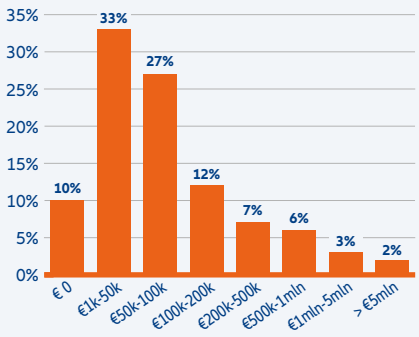
91% van de organisaties die in 2023/2024 te maken had met interne of externe fraude(pogingen) heeft ook daadwerkelijk schade geleden. Van de schades is 55% hoger dan €50.000. 16% hoger dan €200.000. De kans is relatief groot om hard geraakt te worden. Bij interne fraude leidt 2% tot schades hoger dan €1 miljoen. Bij externe fraude is dat 5%

Schadeklap opvangen
Fraude 100% voorkomen is een illusie. Met een fraudeverzekering kunnen organisaties en bedrijven zich beschermen tegen de klap die met (interne of externe) fraude wordt uitgedeeld. Zie meer hierover vanaf pagina 20.

Interne fraude



Externe fraude



3.6. Fraude: 59% doet geen melding bij de politie

Uit onze fraudeonderzoeken blijkt dat bedrijven en organisaties de neiging hebben om steeds vaker een externe partij in te schakelen bij fraude. In het onderzoek van 2022 was dat in 44% van de fraudegevallen, dat steeg vorig jaar naar 75%, en dit jaar naar 80%.

41% van deze groep zegt wel eens bij de politie te hebben aangeklopt vanwege fraude. Dat betekent omgekeerd dat gemiddeld 59% van de fraudegevallen niet wordt gemeld bij de politie. In Nederland is dat 55%, in België 63%.

Het meest wordt een ICT-bedrijf in de arm genomen als er fraude speelt in een organisatie. In België gebeurt dat in de helft van de gevallen, in Nederland bij 36% van de fraudegevallen. Wat opvalt is dat in België vaker een recherchebureau wordt ingeschakeld dan in Nederland (38% vs 27%).

Eén op de vijf bedrijven handelt fraude intern af

3.7. Wat doen organisaties om fraude te voorkomen?

De populariteit van two factor authenticatie is flink gestegen ten opzichte van 2023 (van 39% naar 54%). Over de hele linie worden er in België meer maatregelen genomen dan in Nederland (zoals plaatsen detectie-software en screening medewerkers). Nederlandse organisaties doen vaker aan awareness workshops.

Veiligheidstesten

Steeds vaker worden in beiden landen 'red teaming'-acties uitgevoerd (14%). Externe fraudespecialisten of 'ethical hackers' testen dan in de praktijk hoe gemakkelijk/moeilijk het is om de organisatie binnen te komen en in te breken op de eigen systemen. Belgische bedrijven en organisaties laten vaker penetratietesten uitvoeren om de veiligheid van hun netwerk/systeem te beoordelen (31% vs 16%).

3.8. Kans op fraude neemt verder toe

Fraude is een toenemend risico voor organisaties in het algemeen, meer dan vorig jaar. Daarbij wordt vaak verwezen naar digitalisering en AI. Dit verge-makkelijkt niet alleen fraude, het biedt ook steeds meer (nieuwe) mogelijkheden.

In 2024 vinden meer organisaties dat fraude een toenemend risico is voor organisaties ten opzichte van 2023: 87% vs 81%

Waarom is fraude een toenemend risico?

- "Alles is meer digitaal."
- "Door AI en andere evoluties in de digitale wereld."
- "Door AI is het bijna niet meer te zien wat echt en nep is."
- "Fraudeurs worden steeds slimmer met technologie."
- "De blootstelling aan frauderisico's neemt gestaag toe."
- "Het aantal pogingen lijkt toe te nemen."
- "Omdat er de laatste tijd een toename is van gevallen van hacking en oplichtingspogingen."

Vervolg fraude als toenemend risico

"Bij ons valt het wel mee"

Bijna 90% van de bedrijven en organisaties mag dan vinden dat het frauderisico toeneemt, opvallend is dat men voor de eigen organisatie de toename van het frauderisico veel minder groot acht. Velen denken de juiste maatregelen al genomen te hebben om zichzelf tegen fraude te beschermen. Wat opvalt aan de maatregelen is dat ze vooral digitaal en technisch van aard zijn.

64% vond in 2023 dat fraude een toenemend risico is voor de eigen organisatie. Een jaar later is dat 67%. Van organisaties met meer dan 5000 FTE ziet 58% fraude als een toenemend risico voor zichzelf

Waarom is fraude geen toenemend risico voor uw organisatie?

- "We hebben de juiste beveiliging en een passend beleid om de organisatie te beschermen."
- "De manier van werken en de preventieve maatregelen die genomen worden, dekken dit af."
- "Vertrouwen hebben in de mensheid is belangrijker dan angstzaaien."
- "Goede software in beveiliging."
- "Ik denk dat het risico constant blijft."
- "We hebben een volledig beveiligde omgeving en we blijven de activiteiten van onze medewerkers monitoren."

3.9. Meer bedrijven voeren frauderisicoanalyse uit

Dat de bedrijven fraude als toenemend risico ervaren valt ook op te maken uit het aantal frauderisicoanalyses dat organisaties laten uitvoeren. Dat is verder toegenomen. Hiervoor worden vooral externe uitvoerders voor ingezet (accountant, ICT-bedrijf, adviesbureau, etc.). Kosten houden uitvoering soms nog tegen. De uitgevoerde frauderisicoanalyses hebben voornamelijk betrekking op 'Financiële administratie' en 'Digitaal'.

In 2024 is er vaker een frauderisicoanalyse uitgevoerd dan in 2023: 74% vs 64%

Waarom niet uitgevoerd?

- "Bijna alles wordt intern beheerd."
- "Tot nu toe hebben we weinig te maken gehad met fraude."
- "Het is te duur om te laten uitvoeren."
- "Aanzienlijke kosten."
- "Staat nog op de planning, geen prioriteit gehad."
- "Nog niet bij stil gestaan."

3.10. Thuiswerken verhoogt risico op fraude

Gaf in 2023 50% van de bedrijven en organisaties aan dat thuiswerken het risico op (interne en externe) fraude verhoogt, in 2024 is dat percentage opgelopen naar 55%. In 2022 was dat percentage nog 34%. Het aantal bedrijven dat maatregelen nam is gestegen van 50% tot 61%. Maatregelen die bedrijven nemen liggen vaak in de digitale sfeer (zoals two factor authenticatie, VPN, firewalls en antivirus-software).

Waarom verhoogd risico?

- "Meer toegang van buitenaf."
- "Het 4-ogen-principe wordt minder."
- "De controle is verminderd."
- "Computers op afstand zijn minder controleerbaar (af en toe gebruikt door familie, enz.)."
- "Gebruik van diverse netwerken en gevoelige data."
- "Geen toezicht."
- "Het is riskant vanwege een onbeveiligd netwerk en externe toegang."

Waarom geen verhoogd risico?

- "Omdat het via VPN en firewalls gaat."
- "Werkt via VPN."
- "De laptops van de medewerkers zijn goed beveiligd."
- "De toegang tot gevoelige documenten wordt gecontroleerd."
- "Dezelfde verbinding, beveiliging en handelingen."
- "Medewerkers werken thuis ook vanuit een beveiligde omgeving."
- "Ik heb vertrouwen in medewerkers."

3.11. Komende drie jaar: meer investeringen in fraudepreventie

Ruim een kwart van de bedrijven en organisaties zegt meer te gaan investeren om het frauderisico te beperken. Deze bedrijven steken vooral meer geld in beveiligingsaudits van hun IT-systeem en in trainingen om fraudebewustzijn van medewerkers te vergroten.

Corporate organisaties investeren meer in fraudebewustzijn van medewerkers (66%) dan MKB (45%)

Top 5 investeringen
In de top 5 van investeringen om de schade door fraude te beperken staat ook het afsluiten van een verzekering. In Nederland is dat 22%, in België 30%. Zie voor meer informatie hierover op de volgende pagina's.

Steeds meer bedrijven hebben noodplan
65% van de bedrijven en organisaties zegt dat er een draaiboek/noodplan klaarligt voor het geval er fraude aan het licht komt. In 2023 was dat 58%, in 2022 33%.

3.12. Veel misverstanden over manier van verzekeren tegen fraude

Minder dan de helft van de organisaties beschikt, naar eigen zeggen, over een fraude- (41%), cyber- (34%) of bestuurdersaansprakelijkheidsverzekering (45%). Over de manier van verzekeren tegen fraude hebben bedrijven en organisaties vaak een verkeerd beeld.

45% van de organisaties denkt alle schade door fraude gedekt te hebben met een verzekering. Dat is vaak gebaseerd op een foutieve aanname. Zo zijn er organisaties die ervan uitgaan dat een aansprakelijkheidsverzekering voldoende dekking biedt tegen fraude of dat een kredietverzekering soelaas biedt. Dat is onjuist. Ook over de dekking van een fraudeverzekering en een cyberverzekering bestaan veel misverstanden. Daarnaast speelt ook de bestuurdersaansprakelijkheidsverzekering een rol bij fraude.

Cyberverzekering en fraudeverzekering vullen elkaar aan

Vaak wordt gedacht dat een cyberverzekering beschermt tegen alle digitale fraude. Dit is niet het geval. Neem de schade door een spookfactuur die een fraudeur per email verstuurt; die valt bijvoorbeeld niet onder de cyberverzekering. Omgekeerd dekt een fraudeverzekering niet het losgeld dat geëist wordt om je systemen terug te ontsleutelen waardoor ze opnieuw bruikbaar worden.

Cyberverzekering

De cyberverzekering beschermt organisaties tegen schade door een cyberaanval en tegen aansprakelijkheid voor schade aan derden. Denk aan schade door inbreuk op hun privacy als er data zijn gestolen, schade als er door een hack geheimhouding wordt geschonden, schade door kosten vanwege gestolen data, schade door omzetverlies doordat een organisatie een bepaalde periode niet operationeel is, of schade door cyberafpersing en kosten van het herstel van programmatuur of data.

Fraudeverzekering

Een fraudeverzekering beschermt organisaties voor schade door fraude-rende medewerkers, schade door criminelen die zich voordoen als leverancier of afnemer en zo onterecht goederen of gelden van organisaties verduisteren. Ook kunnen criminelen zich voordoen als medewerkers of zelfs de directeur (CEO-fraude); ook schades die daaruit voortvloeien vallen onder de dekking van een fraudeverzekering. Verder ook de kosten die organisaties moeten maken om systemen te herstellen of imago schade te beperken.

Bijna helft van alle organisaties denkt ten onrechte dat een cyberverzekering voldoende beschermt tegen digitale fraude

Vervolg verzekeringsoplossing

Fraudeverzekering versus cyberverzekering

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

Fraudeverzekering	Cyberverzekering
• (Identiteits)fraude, oplichting, valsheid in geschifte, diefstal door interne medewerkers. • (Identiteits)fraude, oplichting, valsheid in geschifte, diefstal door derden. *Voorbeelden: CEO-fraude, social engineering, deepfake/deepvoice, factuurfraude, fake buyer fraude, het omleiden van betalingsstromen. Maar ook het stelen van wachtwoorden of omleiden naar andere websites in geval er fraude is/wordt gepleegd.* • 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.	• Het kapot maken/platleggen van IT-systemen. • Reparatie/herstelkosten van de systemen. • Bedrijfsschade door een cyberincident (meestal gemaximeerd tot 180 dagen). • Schade voor aansprakelijkheid van het stelen van data (inbreuk op privacy/geheimhouding), kosten intern onderzoek. • Schadevergoeding door uitbetalen van ransom/digitale afpersing. • Cyber diefstal (meestal gemaximeerd tot bijvoorbeeld 50.000 EUR). • Ondersteuning door IT-specialisten in geval van een hack en juridische/forensische ondersteuning.

Aansprakelijkheid van bestuurders

Bestuurders moeten zich volgens de wet maximaal inzetten om risico's te beperken en voorkomen. Dat geldt ook voor het frauderisico. Is daar voldoende aan gedaan? Zo niet, dan zijn bestuurders daarvoor aansprakelijk te stellen als de fraude bijvoorbeeld leidt tot een faillissement.

Uit het onderzoek blijkt dat 41% van de organisaties en bedrijven al een bestuurdersaansprakelijkheidsverzekering hebben afgesloten. 33% geeft aan dit te willen doen.

Bestuurdersaansprakelijkheidsverzekeraars eisen vaker dat organisaties ook een fraudeverzekering afsluiten. Zonder deze verzekering dekken zij niet het hele bestuurdersaansprakelijkheidsrisico meer af.

3.13. Artificial Intelligence zowel kans als bedreiging

In dit onderzoek is het voor het eerst ook ingezoomd op Artificial Intelligence (AI). Bedrijven en organisaties zien het vooral als een positieve ontwikkeling omdat de techniek is te gebruiken om het risico op fraude te verminderen (69% in België, 54% in Nederland). Bijna een kwart van de bedrijven en organisaties zien AI ook als een bedreiging op fraudegebied (27% in Nederland, 21% in België).

Waarom positieve ontwikkeling?

- "Automatisering van bepaalde taken."
- "Data wordt sneller en beter geanalyseerd en gegenereerd."
- "Fraudegevallen sneller aan het licht."
- "Geeft veel meer oplossingsmogelijkheden op heel veel oppervlakken."
- "Verhoogde productiviteit en operationele efficiëntie."
- "Het kan problemen sneller oplossen dan mensen."
- "Het neemt werk uit handen."

Waarom negatieve ontwikkeling?

- "AI heeft in veel fraudegevallen geholpen."
- "Als we overstappen op AI moeten we weer meer uitgeven."
- "Wordt steeds moeilijker om fraude te herkennen."
- "Het wordt moeilijk om waar van onwaar te onderscheiden."
- "Kan misbruik veroorzaken."
- "Door AI zijn/komen er meer manieren om te fraude-ren en wordt het ook praktisch om uit te voeren."

Conclusies

1 In 2023 vond 85% van de bedrijven en organisaties de bescherming tegen fraude (ruim) voldoende. In 2024 is dit opgelopen naar 91%. Nederlandse organisaties zijn nog tevredener over de eigen bescherming dan Belgische: 95% vs 85%. Er lijkt hier sprake van een vals gevoel van veiligheid. Ruim tweederde van de bedrijven en organisaties had in de onderzoeksperiode te maken met interne of externe fraude(pogingen). 91% hiervan leidde tot daadwerkelijke schade.

2 Het beeld dat in het onderzoek van 2024 nadrukkelijk naar voren komt is dat bedrijven en organisaties in toenemende mate vooral technische maatregelen nemen om fraude te voorkomen. Het resultaat hiervan is dat het aantal gevallen van waargenomen fraude(pogingen) met 10% is gedaald in de periode 2023-2024 (phishing is hierbij niet meegenomen). Het idee dat met enkele technische maatregelen het fraudeprobleem afdoende is opgelost is onterecht.

3 Ontvreemding van goederen komt het vaakst voor bij interne fraude, terwijl factuurfraude de meest voorkomende vorm van externe fraude is. In de meeste gevallen heeft fraude een kleine impact op organisaties, maar bij één derde is de impact aanzienlijk. In financiële termen is 55% van de fraudeschades hoger dan €50.000. 16% hoger dan €200.000.

4 Bedrijven en organisaties schakelen steeds vaker een externe partij in bij fraude (in 2024 80%). 41% van deze groep zegt wel eens bij de politie te hebben aangeklopt vanwege fraude. Dat betekent omgekeerd dat gemiddeld 59% van de fraudegevallen niet wordt gemeld bij de politie. In Nederland is dat 55%, in België 63%.

5 Interne fraude wordt vooral door mannen gepleegd (75%). Vaak mannen die minder dan vijf jaar in dienst zijn, in de leeftijdscategorie 26 tot 45 jaar. Kijken we naar de hoogte van de schadelast dan veroorzaken leden van directie en management bij interne fraude de hoogste schadeposten.

6 Fraude wordt vaker gezien als een toenemend risico. Men wijt dit vooral aan digitalisering en AI, waardoor fraude steeds makkelijker wordt. Voor de eigen organisatie wordt fraude echter minder vaak als een toenemend risico gezien, omdat men denkt de juiste maatregelen al genomen te hebben. Zo worden frauderisicoanalyses vaker gedaan in 2024 (hoewel kosten de uitvoering hiervan soms nog tegenhouden). Het thuiswerken verhoogt volgens velen het risico op fraude, omdat er minder toezicht en controle is op werknemers. Men nam in 2024 dan ook meer maatregelen om het risico van thuiswerken te verminderen.

7 Een kwart van de organisaties is van plan om de komende drie jaar meer te gaan investeren in het voorkomen van fraude en oplichting. Hierbij denkt men vooral aan een beveiligingsaudit IT, het vergroten van het intern bewustzijn of een audit ter versterking van de interne administratieve procedures. Het merendeel van de organisaties heeft een draaiboek/ noodplan beschikbaar voor het geval ze met fraude te maken krijgen. De directie en de juridische afdeling zijn daarbij vaak leidend.

8 Minder dan de helft van de organisaties beschikt, naar eigen zeggen, over een fraude-, cyber- of bestuurdersaansprakelijkheidsverzekering. Over de verzekeringsoplossing voor fraudeproblemen bestaan veel misvattingen. 45% van de organisaties denkt alle schade door fraude gedekt te hebben met een verzekering. Als daarop wordt ingezoomd blijkt het vaak om foutieve aannames te gaan.

9 Artificial Intelligence wordt over het algemeen als een positieve ontwikkeling gezien dat het risico op fraude vermindert. Het versnelt procedures en neemt werk uit handen. Sommigen vinden dat AI juist misbruik kan veroorzaken.

Wil je meer weten over onze oplossingen van kredietverzekering, garantie of fraudeverzekering? Neem contact op met ons team.

+31 (0)73 306 06 03

advies@allianz-trade.com

www.allianz-trade.nl

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

Euler Hermes Nederland
Kantoor 's-Hertogenbosch, Brabantlaan 2, 5216 TV 's-Hertogenbosch, Tel. 0800 - 385 37 65, contactnl@allianz-trade.com
Kantoor Amsterdam (Garanties), De Entree 31 (Alpha Tower), 1101 BH Amsterdam-Zuidoost, Tel. 020 - 696 39 41, garanties@allianz-trade.com
www.allianz-trade.nl

Euler Hermes Nederland, Euler Hermes Garanties en Euler Hermes Kredietverzekering zijn handelsnamen van Euler Hermes NV, Kunstlaan 56, BE-1000 Brussel, BTW BE 0403.248.596 RPM Brussel, Verzekeringsonderneming toegelaten onder code 418.