Allianz Trade

TRENDRAPPORT 2023

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 zijn de belangrijkste misvattingen over fraude?

1. Inleiding 4
2. Verantwoording 5
3. De resultaten 6
   - 3.1. Interne fraude 8
   - 3.2. Externe fraude 9
   - 3.3. Interne fraudeurs: vaak mannen die kort in dienst zijn 11
   - 3.4. 15% van fraudeschades ligt boven de €200.000 12
   - 3.5. Fraude: vaak niet gemeld bij politie 13
   - 3.6. Wat doen organisaties om fraude te voorkomen? 14
   - 3.7. Organisaties zien vooral digitale kwetsbaarheid toenemen 15
   - 3.8. Meer bedrijven voeren frauderisicoanalyse uit 16
   - 3.9. Thuiswerken: meer risico op fraude 18
   - 3.10. Komende drie jaar: meer investeringen in fraudepreventie 20
   - 3.11. Veel misverstanden over manier van verzekeren tegen fraude 21

Conclusies 23

1. Inleiding

Allianz Trade is expert op het gebied van fraude. In navolging van onze fraudeonderzoeken in andere landen is in 2022 voor het eerst een fraudeonderzoek uitgevoerd in Nederland en België. In 2023 hebben we dit onderzoek opnieuw uitgevoerd. Dit 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 fraudeontwikkelingen te registreren. Aanvullend beoogt het onderzoek ook inzicht te geven in de verzekerbehoefte van bedrijven en organisaties op fraudegebied.

2. Verantwoording

In opdracht van Allianz Trade is het onderzoek in het voorjaar van 2023 uitgevoerd door MetrixLab. In totaal werkten 355 bedrijven/organisaties mee aan dit onderzoek (200 in Nederland, 155 in België). 48% betreft B2B-bedrijven, 35% B2C en 17% 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. De top 5 van branches die het meest zijn vertegenwoordigd ziet er als volgt uit: financiële dienstverlening 17%, ICT 17%, overheid 12%, bouw/installatie 9% en zakelijke dienstverlening 9%.

Allianz Trade
's-Hertogenbosch / Brussel, juni 2023

3. De resultaten

Uit het onderzoek blijkt dat 79% van de organisaties recent te maken heeft gehad met interne of externe fraude(pogingen). Van deze 79% leed een meerderheid ook daadwerkelijk schade.

Ook al bevestigt een ruime meerderheid dat ze slachtoffer waren van fraude en schade leden, toch geeft 84% aan dat ze van zichzelf vinden dat ze (ruim) voldoende beschermd zijn. Hier lijkt sprake van een onterecht gevoel van veiligheid. Men is niet goed beschermd, maar men voelt zich goed beschermd. Wat hierbij meespeelt is dat veel organisaties de eigen vuile was liever niet buiten hangen.

Van alle organisaties die te maken kregen met interne en externe fraude(pogingen), leed een meerderheid ook daadwerkelijk schade.

Vooral vrees voor het verlies van (online) gegevens

Waar maken organisaties zich het meest zorgen om als ze te maken krijgen met fraude en oplichting? Een grote meerderheid vreest vooral het verlies van (online) gegevens en andere vormen van cybercriminaliteit:

- “Een van mijn grootste zorgen is dat hackers toegang zouden kunnen krijgen tot de bedrijfsdatabase.”
- “Schade aan reputatie en de financiële gevolgen daarvan.”
- “Cybercriminaliteit.”
- “Gebrek aan kennis medewerkers. Teveel vertrouwen.”
- “Phishing mails, oplichting, werknemers die frauderen.”
- “Ontvreemding van spullen en of intellectueel eigendom.”
- “Computerhacking waarvoor losgeld vereist is.”

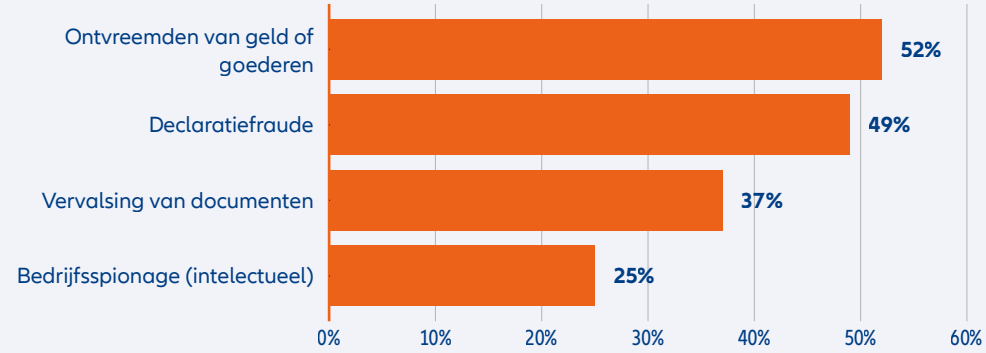
Wat verstaan we onder (interne en externe) fraude?

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 van nieuwe technologieën op het gebied van digitale fraudes (zoals deepvoice/deepfake/nep e-mails).

3.1. Interne fraude

Hoewel veel aandacht in de media uitgaat naar cybercrime wordt juist ook veel fraude gepleegd door eigen werknemers.

DE TOP 4 VAN DE MEEST VOORKOMENDE INTERNE FRAUDE



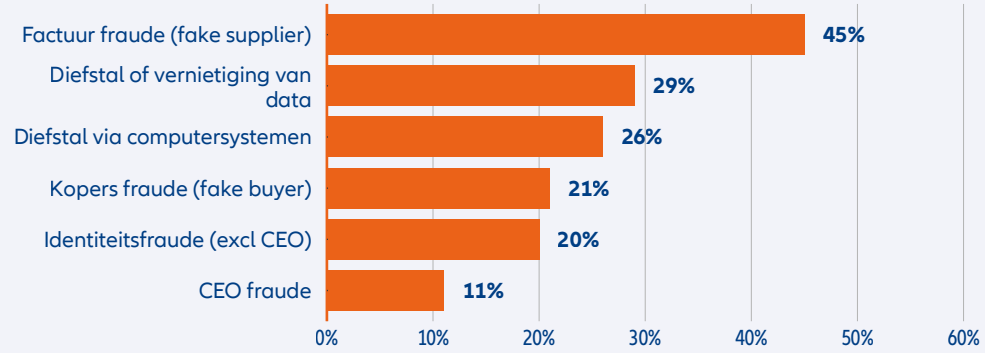
Hierbij valt op dat declaratiefraude duidelijk meer in Nederland voorkomt dan in België (56% vs 38%)

Bij interne fraude gaat het vooral om ontvreemding van geld of goederen en declaratiefraude.

3.2. Externe fraude

Bij externe fraude komt veruit het meest voor dat er valse facturen worden verstuurd.

MEEST VOORKOMENDE EXTERNE FRAUDE



Fake buyer fraude
Bij fake buyer fraude doet een oplichter zich voor als een (bestaande) klant. De fake buyer 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).

Fake supplier fraude
Bij fake supplier fraude doet de oplichter alsof hij goederen/diensten heeft geleverd (wat niet het geval is) en stuurt daarvoor een factuur. Denk daarbij ook aan voorschotfraude waarbij de fraudeur om vooruitbetaling vraagt. De spookfacturen zijn nauwelijks van echte facturen te onderscheiden. Vaak is alleen het bankrekeningnummer (en de tenaamstelling) afwijkend. Bij deze valse facturen gaat het in veel gevallen om relatief kleine bedragen. De oplichter hoopt dat de spookfactuur in de dagelijkse drukte op de administratieafdeling 'blindelings' wordt afgehandeld.

Identiteitsfraude
Bij identiteitsfraude doen criminelen zich voor als iemand anders (bijvoorbeeld alsof ze klant of collega zijn). In Nederland doet identiteitsfraude zich duidelijk vaker voor dan in België (29% vs 8%). Als de fraudeur doet alsof hij de directeur is wordt het CEO-fraude genoemd.

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. Interne fraudeurs: vaak mannen die kort in dienst zijn

Interne fraude wordt aanmerkelijk vaker door mannen dan door vrouwen gepleegd (64% vs 20%). Het zijn vaak mannen die minder dan vijf jaar in dienst zijn.

Op welke afdelingen wordt het meest gefraudeerd?
Het hoogst scoort Finance met 36%. Op de tweede plaats Commercie, waarbij opvalt dat in België op deze afdeling vaker fraude wordt gepleegd dan in Nederland (34% vs 14%). Op de derde plaats staat Operations met 26%.

Langer in dienst? Minder kans op fraude
Naarmate mannen langer in dienst zijn, neemt de kans op interne fraude af. Interne fraudeurs zijn vaak relatief kort in dienst (1 tot 5 jaar).

In 36% van de gevallen is fraudeur werkzaam op Finance-afdeling.

3.4. 15% van fraudeschades ligt boven de €200.000

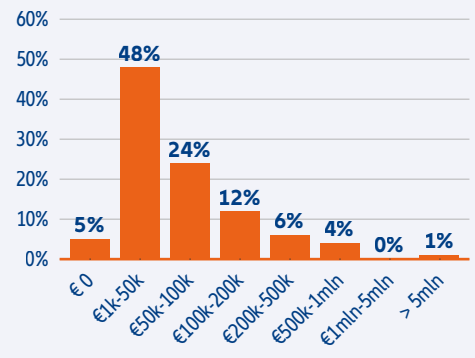
Bijna de helft van de fraudeschades ligt tussen de €1 en €50.000. In deze categorie valt op dat de schadeposten bij interne fraude vaak hoger uitvallen dan bij externe fraude.

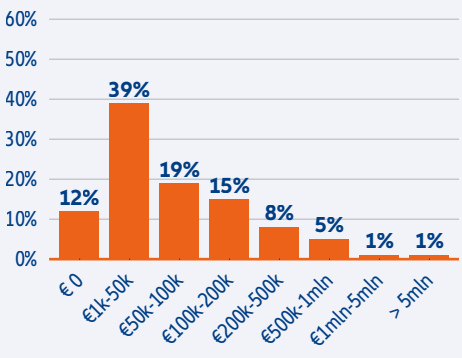
In ruim 20% van de fraudegevallen is er sprake van €50.000 tot €100.000 schade. 12% tussen €100.000 en €200.000. 15% van de schades bedraagt meer dan twee ton, waarvan 4% tussen €500.000 en €1.000.000. Bij 1% meer dan €5.000.000.

Met een fraudeverzekering is de grote impact van fraude af te dekken.

Van alle organisatie die met interne of externe fraude(pogingen) te maken hadden, leed een meerderheid ook daadwerkelijk schade.

GELEDEN SCHADE





3.5. Fraude: vaak niet gemeld bij politie

Driekwart van de organisaties die met fraude te maken kreeg, heeft eens of vaker externe partners ingeschakeld om fraude te stoppen dan wel af te handelen. Bijna de helft van deze groep (43%) zegt wel eens bij de politie te hebben aangeklopt hiervoor. Dat betekent omgekeerd dat 57% van de fraudegevallen niet wordt gemeld bij de politie.

In België vaker advocaat ingeschakeld
Het meest wordt een ICT-bedrijf in de arm genomen als er fraude speelt in een organisatie. Wat opvalt is dat in België vaker een advocatenkantoor wordt ingeschakeld dan in Nederland (43% vs 20%). In België wordt überhaupt meer hulp ingeschakeld (84% vs 68%). Nederlandse organisaties lossen het vaker intern, op eigen houtje op (in 32% van de gevallen).

Meer externe hulp ingeroepen dan in 2022
In vergelijking met het fraudeonderzoek van 2022 hebben bedrijven en organisaties de neiging om sneller een externe partij in te schakelen. In het vorige onderzoek zei 44% wel eens externe hulp in te schakelen. Dat percentage is nu 75%.

Eén op de vier bedrijven handelt fraude intern af.

3.6. Wat doen organisaties om fraude te voorkomen?

Welke methodes gebruiken organisaties om interne en externe fraude te voorkomen? Meest genoemd zijn maatregelen als fraudebewustzijn van medewerkers vergroten, extra controle vanuit de administratieve organisatie en screening van medewerkers. Kijken we naar andere maatregelen dan valt op dat Nederlandse organisaties vaker dan in België gebruik maken van two factor authenticatie en het vierogenprincipe.

Veiligheidstesten
In België laten organisaties vaker penetratietesten uitvoeren om de veiligheid van hun netwerk/systeem te beoordelen. Ook zetten ze vaker 'red teaming'-acties in waarbij ze een externe fraudespecialist of hacker in de praktijk laten testen hoe gemakkelijk/moeilijk het is om de organisatie binnen te komen en in te breken op de eigen systemen.

Organisaties met meer dan 1000 werknemers maken relatief vaker gebruik van workshops en tools om de oplettendheid van de medewerkers te vergroten.

Het zijn vooral grote organisaties die actie ondernemen om fraude te voorkomen en te detecteren.

3.7. Organisaties zien vooral digitale kwetsbaarheid toenemen

De meerderheid van de organisaties ziet fraude als een toenemend risico in het algemeen. Als oorzaak noemen ze digitalisering, automatisering en nieuwe technologie. Maar ook hier geldt weer dat men het risico meer voor de 'buurman' ziet dan voor zichzelf (zie begin hoofdstuk 3). Vooral bij minder grote bedrijven wordt gemakkelijk gedacht 'bij mij gebeurt het niet' of 'ik ken mijn medewerkers' of 'onze firewall is goed genoeg'. Driekwart van de grote bedrijven (meer dan 5000 FTE) ziet fraude wel als een toenemend risico voor zichzelf.

- "Digitalisering zorgt voor meer mogelijkheden om fraude te plegen."
- "Ik denk dat in de groeiende online markt en vooral het gebrek aan kennis hiervan bij de oudere generaties zorgt voor een groter wordend risico op oplichting en phishing."
- "Er zijn heel veel rechtstreekse mails naar medewerkers met telkens links en toegangen tot ons netwerk."
- "Men wordt steeds slimmer en technologie wordt ook voor criminelen geavanceerder."
- "Alles gaat digitaal en dat is goed maar wel heel erg fraudegevoelig."
- "IT en automatisering vergemakkelijken het werk, maar ook fraude. De stroom aan gegevens wordt zo groot dat het moeilijk is om deze te controleren."

3.8. Meer bedrijven voeren frauderisicoanalyse uit

Dat de bedrijven fraude als toenemend risico ervaren valt ook op te maken uit het aantal fraude-risicoanalyses dat organisaties laten uitvoeren. 64% van de organisaties zegt dat te doen (in het onderzoek van vorig jaar bedroeg dat percentage 37%). Organisaties schakelen hiervoor partijen in als ICT-bedrijven, interne teams, externe advies-bureaus en accountantsbureaus.

Op de vraag waarom bedrijven geen frauderisicoanalyse uitvoerden volgen antwoorden als:

- "Urgentie lag niet hoog genoeg, omdat het preventief is."
- "Wij zien geen toegevoegde waarde. De fraudes waar wij mee te maken hebben gekregen, worden niet gestopt door dit soort analyses."
- "Geen financiële middelen."
- "We doen het intern door onze eigen ICT en auditafdeling."

Frauderisicoanalyses zijn vooral gefocust op digitale fraude en financiële adminis-tratie.


MATCHING
MATCHED
ID 96421654174
Hashcode RTY4 1DSE BTW4 ZWQ1
##READING .....
/:FSGKLJJ33 13244%#S 1315FHRS A3124#31D14412D
/:31245FFR44 %#3110 0134
/:AW3232FGG8##3214 FGTG;J1134
/:32132144HSD %%PKKKJ 13444881 ZAZ3
/:JSFE1134 841%S11 #32144
/:JUDJ434% GLK##::AA7 S4777431145 8SFR 1
/:OO1001 ASW475#7414 SSFE% FGJJJ1154 314845
/:SDW31115 1AS5WD11 S2QQQ11 S2213%A #ZS411
ACCESS GRANTED
##READING .....
/:FSGKLJJ33 13244%#S 1315FHRS A3124#31D14412D
/:31245FFR44 %#3110 0134
/:AW3232FGG8##3214 FGTG;J1134
/:32132144HSD %%PKKKJ 13444881 ZAZ3
/:JSFE1134 841%S11 #32144
/:JUDJ434% GLK##::AA7 S4777431145 8SFR 1
/:OO1001 ASW475#7414 SSFE% FGJJJ1154 314845
/:SDW31115 1AS5WD11 S2QQQ11 S2213%A #ZS411

3.9. Thuiswerken: meer risico op fraude

Corona ligt nu bijna twee jaar achter ons. Thuiswerken is gemeengoed geworden. En volgens de respondenten is daardoor het risico op fraude toegenomen. 50% van de bedrijven antwoordt met 'ja' op de vraag of thuiswerken door medewerkers het risico op interne en externe fraude voor de organisatie heeft vergroot. Vorig jaar was dat percentage nog 34%.

Gevoeliger voor fraudeurs

Hierbij gaat het niet alleen om interne fraude, bijvoorbeeld tijdsfraude/declaratiefraude (minder controle mogelijk bij thuiswerken) maar ook om externe fraude. Medewerkers die 'geïsoleerd' thuiswerken zijn gevoeliger voor fraudeurs. Op het werk is het gemakkelijker om bij twijfel een collega te raadplegen die in dezelfde ruimte werkt.

Hoezo verhoogt thuiswerken het frauderisico?

- "Hoe je het ook wendt of keert, er is gewoon minder controle op wat mensen thuis doen. Dus een hoger risico op fraude."
- "De beveiliging thuis is minder goed dan op kantoor."
- "Je mist op dat moment soms een extra controle als iemand bijvoorbeeld twijfelt, kan je niet even meekijken. Daarnaast gebeurt nu steeds meer digitaal wat ook een extra risico met zich meebrengt."
- "Er is minder overzicht op medewerkers en ze hebben dus grotere kans om te frauderen."
- "We werken volgens uurloon, er valt niet te checken of bijvoorbeeld de daadwerkelijk contractuele uren gemaakt worden."

50% van de organisaties zegt dat thuiswerken het risico op interne en externe fraude verhoogt.

Veel organisaties nemen maatregelen in digitale sfeer

Van alle organisaties die thuiswerken als verhoogd risico zien (50%), heeft 68% maatregelen genomen. Het gaat daarbij vooral om maatregelen in de digitale sfeer.

Wat is er aangepast?

- "Two factor authenticatie."
- "VPN."
- "Firewalls en antivirus."
- "We hebben heel wat websites geblokkeerd. Https is een must en ingesteld."
- "Antivirus en e-mail bescherming regelmatig updaten."

Organisaties die geen maatregelen nemen, zeggen:

- "Het wordt niet gezien als een verhoogd risico."
- "Geen financiële middelen."
- "Het is niet nodig geweest."
- "Er moet nog verder naar gekeken worden."
- "Betrouwbare medewerkers in het bedrijf."

3.10. Komende drie jaar: meer investeringen in fraudepreventie

Bijna dertig procent van de 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.

Top 5 investeringen
In de top 5 van investeringen om de schade door fraude te beperken staat ook het afsluiten van een verzekering vermeld. Wat opvalt is dat in België 32% van de organisaties hiervoor kiest, in Nederland 16%.

Steeds meer bedrijven hebben noodplan
In 2022 zei 33% van de organisaties dat ze een draaiboek / noodplan hadden klaarliggen voor het geval er fraude aan het licht zou komen. Dat percentage is in een jaar tijd gegroeid naar 58%.

58% heeft een draaiboek / noodplan achter de hand.

3.11. Veel misverstanden over manier van verzekeren tegen fraude

49% van de organisaties denkt alle schade door fraude gedekt te hebben met een verzekering. Dat is 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.

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 frauderende 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 de helft van alle organisaties denkt ten onrechte dat een cyberverzekering voldoende beschermt tegen digitale fraude. Als sluitstuk voor hun risicopreventie kunnen bedrijven naast cyberverzekering, kredietverzekering en bedrijfsaansprakelijkheidsverzekering een fraudeverzekering afsluiten voor het geval dat preventieve maatregelen onvoldoende bleken te zijn.

Meer Belgische organisaties zijn van plan zich te verzekeren dan Nederlandse organisaties (35% vs 25%).

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 geschrifte, diefstal door interne medewerkers. • (Identiteits)fraude, oplichting, valsheid in geschrifte, diefstal door derden. *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.* • 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 48% een bestuurdersaansprakelijkheidsverzekering heeft afgesloten. 29% 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.

Conclusies

1 Er bestaat een onterecht gevoel van bescherming en veiligheid rond fraude. 84% vindt zich (ruim) voldoende beschermd tegen fraude en oplichting. Men voelt zich beschermd maar in de praktijk krijgt 79% van de organisaties te maken met interne of externe fraude(pogingen). Een meerderheid hiervan lijdt ook schade.

2 De grootste zorgen van organisaties m.b.t. fraude en oplichting zijn het verlies van (online) gegevens en andere vormen van cybercriminaliteit.

3 Driekwart van de organisaties heeft een keer gebruik gemaakt van een externe partner bij het detecteren of afhandelen van fraude/oplichting. In het merendeel van de fraudegevallen slagen organisaties erin om het intern te detecteren of af te handelen.

4 Interne fraude wordt aanmerkelijk vaker door mannen dan door vrouwen gepleegd (64% vs 20%). Het zijn vaak mannen die minder dan vijf jaar in dienst zijn.

5 15% van fraudeschades ligt boven de €200.000. Bijna de helft van de fraudeschades ligt tussen de €1 en €50.000. In deze categorie met de 'laagste' schades valt op dat de schadeposten bij interne fraude vaak hoger uitvallen dan bij externe fraude (48% vs 39%).

6 Fraude wordt vaak niet gemeld bij politie. Van de organisaties die met fraude te maken hebben, meldt 57% dit niet bij de politie.

7 Risico op fraude door thuiswerken is toegenomen. 50% van de bedrijven antwoordt met 'ja' op de vraag of thuiswerken door medewerkers het risico op interne en externe fraude voor de organisatie heeft vergroot. Vorig jaar was dat percentage nog 34%.

8 Bijna dertig procent van de organisaties zegt meer te gaan investeren om het frauderisico te beperken. De populairste investeringen zijn beveiligingsaudits van de IT en het vergroten van het interne bewustzijn. Verder heeft meer dan de helft van de organisaties al een noodplan.

9 Er bestaan veel misverstanden over verzekeringen die de schade van fraude opvangen. Veel organisaties denken ten onrechte dat ze alle fraudeschade (van diefstal tot cybercrime) afgedekt hebben.

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

+31 (0)73 306 06 0

contactnl@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.