WEERBAAR EN WAAKZAAM

Grip op fraude, criminaliteit en cyberdreigingen in een ongrijpbaar tijdperk

VERBOND VAN VERZEKERAARS

Inhoudsopgave

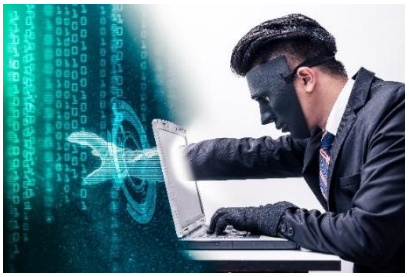
Deze visie is opgesteld door het Centrum Bestrijding Verzekeringscriminaliteit (CBV) van het Verbond van Verzekeraars (oktober 2025).

Het Verbond ondersteunt via het CBV verzekeraars bij het aanpakken en voorkomen van verzekeringsfraude en -criminaliteit en bij hun eigen cybersecurity – zowel door beleidsontwikkeling voor de sector als operationele dienstverlening aan verzekeraars.

Inleiding

Verzekeraars zijn in Nederland een rotsvast gegeven. Mensen die zorgeloos willen leven, ontwikkelen en ondernemen, rekenen erop zekerheid te vinden in een vertrouwde en bovenal veilige verzekeringsmarkt. Zeker in deze tijd is dat vertrouwen een groot goed. Ingrijpende maatschappelijke en revolutionaire technologische veranderingen voltrekken zich in een bijna onnavolgbaar tempo. Dit leidt tot kansen, maar ook tot groeiende onzekerheid en een steeds grilliger risicolandschap. Helaas gedijen fraudeurs, (cyber)criminelen en andere kwaadwillende actoren goed in deze omstandigheden.

Het Centrum Bestrijding Verzekeringscriminaliteit (CBV) van het Verbond signaleert dat niet alleen verzekerden met snel innoverende criminelen te maken krijgen. Verzekeringsbedrijven, -producten, -processen en -ketens zélf zijn steeds vaker een doelwit van onrechtmatig handelen. Gefaciliteerd door nieuwe digitale netwerken, kanalen en toepassingen zijn pogingen tot misbruik of inbreuk inmiddels aan de orde van de dag. Verzekeraars staan de komende jaren voor grote uitdagingen om hun klanten en zichzelf te beschermen en grip te houden op de impact van criminaliteit op hun bedrijfsvoering.



De geschiedenis bewijst gelukkig dat onze sector goed in staat is om in te spelen op veranderende omstandigheden rond criminaliteitsrisico's en de aanpak daarvan. Dit blijkt ook uit de review door het CBV op het vorige visiedocument 'Data en daadkracht' uit 2020 en de daarvoor gevoerde gesprekken met verzekeraars, experts en publieke stakeholders. Hieruit komt het beeld naar voren dat verzekeraars de afgelopen vijf jaar werk hebben gemaakt van de in 2020 beoogde veranderingen. Verzekeraars hebben de destijds aangegeven actielijnen vertaald naar eigen strategieën en beleid. En sectorbreed is sprake van merkbare versterking op het terrein van preventie, informatiedeling, samenwerking, de inzet van technologie en de aanpak van georganiseerde bendes.

De afgelopen vijf jaar:

- Hebben verzekeraars 54.000 gevallen van verzekeringsfraude gedetecteerd. Dat is 5% meer dan de vijf jaar daarvoor.
- Hebben verzekeraars hun cybersecurity versterkt door ruim 950 keer operationele (dreigings)informatie met elkaar te delen.

De wedloop met criminelen houdt daarmee natuurlijk niet op. De geraadpleegde bronnen en respondenten laten er geen twijfel over bestaan dat veel ontwikkelingen die momenteel plaatsvinden een dusdanig grote impact hebben dat een nieuwe visie op de aanpak van uiteenlopende criminaliteitsrisico's die de sector zélf kunnen raken noodzakelijk is.[1] Daarbij hechten externe partijen veel waarde aan een actueel document waarin de collectieve inzet van verzekeraars in dit kader staat beschreven. Maar het zijn vooral verzekeraars zélf die – met het vizier op 2030 – vragen om nieuwe richtinggevende inzichten en *calls-to-action* vanuit het Verbond. Onderliggend is de behoefte om de hele organisatie zo 'mee te kunnen krijgen' in de extra stappen die nodig zijn om kwaadwillenden óók in de toekomst effectief het hoofd te kunnen blijven bieden.

Voor u ligt het gewenste nieuwe visiedocument. Hierin zijn dit keer ook de meerjarige ambities van het Verbond en het CBV opgetekend om verzekeraars te ondersteunen bij de uitvoering van de *calls-to-action* en het verwezenlijken van de visie-doelstellingen. Om hierin succesvol te zijn, moeten verzekeraars over de gehele linie werk maken van verbinding. Verbinding onderling en binnen de verzekeringsketen, verbinding met samenleving, technologie en verbinding tussen publieke en private partijen.

Opgaven in criminaliteitsaanpak: vizier op 2030

Op een ochtend in 2030 worden we wakker. Kant-en-klare hulpmiddelen, gebaseerd op kunstmatige intelligentie (AI), hebben ons dagelijks leven in diverse opzichten makkelijker gemaakt. Tegelijkertijd worden we aan de lopende band met verhulde digitale dreigingen geconfronteerd. Door de wijdverspreide beschikbaarheid van dezelfde AI-tools, is het voor eenlingen een koud kunstje om frauduleuze praktijken

[1] (Verzekerde) criminaliteitsrisico's, alsook bredere bedrijfsvoering-vraagstukken voor verzekeraars, bijvoorbeeld in relatie tot toezicht en relevante wet- en regelgeving op het terrein van informatiebeveiliging, vallen nadrukkelijk buiten de scope van deze visie.

en cyberaanvallen te professionaliseren, te automatiseren en op te schalen. De capaciteiten van criminele netwerken zijn hierin nog velen malen groter. In de obscuriteit van het online landschap lijkt de pakkans zo goed als nihil. De vereiste expertise bij publieke en private partijen in het veiligheidsdomein blijft vaak mijlenver achter.

Het is ook voor verzekeraars een realistisch, maar niet onoverkoombaar, scenario. Verzekeringsfraude en -criminaliteit zijn de afgelopen tijd goeddeels verschoven naar digitale bedrijfsprocessen en het cyberdomein. Criminaliteitsrisico's dienen zich steeds vaker aan via partijen in de keten. Deze ontwikkelingen maken het belangrijker dan ooit dat verzekeraars hun preventieve inspanningen opvoeren, hun digitale weerbaarheid versterken en proactief optreden tegen ondermijnende activiteiten in de samenleving en in de keten.

Cruciaal bij dit alles blijft het vermogen om het verschil tussen nep en echt in een zo vroeg mogelijk stadium te herkennen. Hiervoor moeten verzekeraars nieuwe technologieën en mogelijkheden tot dataverzameling ten volle benutten, maar hun medewerkers wel als de sterkste schakel blijven zien en faciliteren. Mensen die bij verzekeraars werken blijven ook onmisbaar in de vertrouwensrelatie met klanten en de samenleving als geheel. Die samenleving kijkt kritischer dan voorheen naar private partijen die hun verantwoordelijkheid nemen om fraude en criminaliteit actief aan te pakken.

De grote opgave voor verzekeraars blijft om schade door criminaliteit aan de eigen bedrijfsvoering en ten koste van hun klanten en relaties zo veel mogelijk terug te dringen. Hiervoor is het op alle fronten nodig om de handen ineen te slaan, helder te communiceren, informatie en kennis te delen. Bij dit laatste gaat het niet alleen om leren van elkaars oplossingen, maar ook van elkaars slechte ervaringen. Met dit in gedachten wil het CBV de komende jaren, samen met de leden, inzetten op:

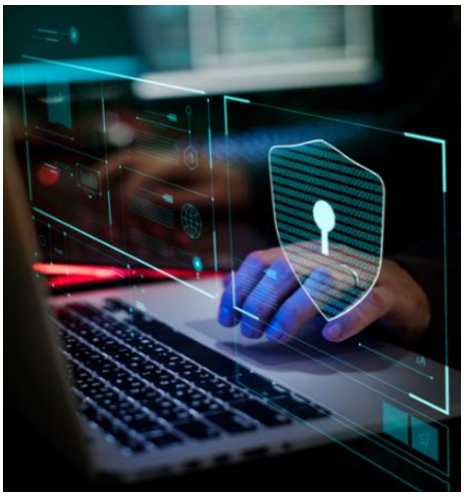
1. Versterking van preventie en weerbaarheid
2. Verhoging van risicobewustzijn en alertheid
3. Verantwoorde omgang met mensen, data en technologie
4. Optreden tegen criminaliteitsrisico's in de samenleving en de keten
5. Oplossingen voor effectieve en kostenefficiënte maatregelen

1. Preventie en weerbaarheid

Zeker in een steeds complexere en veeleisende bedrijfsomgeving is het voorkomen van schade door fraude en criminaliteit beter dan genezen. Slimme preventiemaatregelen worden op de achtergrond doorgevoerd met het doel om fraude- en criminaliteitsrisico's gericht buiten de deur te houden. Goedwillende (aspirant) klanten hoeven dan weinig drempels in online dienstverlening, claim- of aanvraagprocessen te ervaren. Integendeel; denken over preventie levert vaak kansen op om interne processen en 'customer journeys' nog efficiënter en gebruiksvriendelijker in te richten. Door het veiligheids-serviceniveau zichtbaar te maken kan de verzekeraar bovendien extra vertrouwen winnen van een consument die zelf ook steeds meer op zijn hoede is.

Als gevolg van de toenemende mogelijkheden voor individuen om criminele praktijken te professionaliseren, verwatert het klassieke onderscheid tussen opportunistisch en meer georganiseerd frauduleus gedrag. Veelvoorkomende 'kleine' verzekeringsfraude is hierdoor minder goed dan voorheen tegen te gaan door middel van afschrikking – zeker als de perceptie van de pakkans laag blijft. Inzichten hieromtrent zijn bovendien aan verandering onderhevig. Uit onderzoek blijkt dat positieve, normbevestigende communicatie mogelijk meer effect heeft op het voorkomen van gelegenheidsfraude dan negatieve.

In het huidige tijdperk laten de meer georganiseerde fraudeurs en (cyber)criminelen zich sowieso niet snel afschrikken. Vanuit een toenemend gevoel van anonimiteit en onaantastbaarheid zullen zij, linksom of rechtsom, doorlopend proberen om bij verzekeringsorganisaties 'binnen te komen'. Als zij hierin slagen kan de financiële, maatschappelijke en reputationele impact groot zijn. Verzekeraars moeten daarom nog meer in het werk stellen om hun (digitale) voordeur dicht te houden.



Realiteit is dat zwakke plekken in de bedrijfsvoering van verzekeraars soms jarenlang onopgemerkt blijven. Er zijn ook voorbeelden van zwakke plekken waarvan al langer bekend is dat ze actief door kwaadwillenden worden uitgebuit, maar die om uiteenlopende redenen niet afdoende worden aangepakt. Meer snelheid en daadkracht bij preventie is richting de toekomst van groot belang.

Hoewel de dagelijkse verantwoordelijkheid voor het detecteren, onderzoeken en opvolgen van incidenten en kwetsbaarheden hoofdzakelijk bij veiligheids- en cybersecuritymedewerkers ligt, komen effectieve interventies steeds vaker pas tot stand als deze medewerkers buiten de grenzen van het eigen vakgebied treden. Samenwerking met partijen met specialistische kennis of 'eigenaarschap' over de omgevingen waarbinnen ingrepen gevraagd zijn, is dan noodzakelijk.

Ook kan het van grote waarde zijn om preventietrajecten multidisciplinair aan te vliegen door partijen van buiten de sector actief te betrekken. Hiervoor is lef en initiatief van de zijde van de verzekeraar nodig.

- ➔ Verzekeraars maken hun eigen cybersecurity tot een prioriteit.
- ➔ Verzekeraars stellen alles in het werk om kwetsbaarheden in producten, processen en systemen te voorkomen, zo snel mogelijk te signaleren en te verhelpen – en delen de ervaringen en 'lessons learned' structureel met elkaar.
- ➔ Verzekeraars hanteren bij het ontwikkelen van preventieve maatregelen, waar nodig, een organisatiebrede en multidisciplinaire aanpak.

- ➔ Het Verbond zorgt via ledencommunicatie en zelfregulering voor extra aandacht in de bestuurskamers van verzekeraars voor weerbaarheid tegen digitale fraude en cybercriminaliteit.
- ➔ Het Verbond onderhoudt en creëert waar nodig nieuwe kanalen en platforms waardoor verzekeraars relevante ervaringen en (preventieve) kennis nóg sneller en effectiever met elkaar kunnen delen, op een verantwoorde en waar nodig vertrouwelijke wijze.
- ➔ Het Verbond genereert, waar effectief, publiciteit met publieke en private partners rond successen in de aanpak van fraude en criminaliteit om zo gezamenlijk krachtige preventieve signalen aan de samenleving af te geven.

2. Risicobewustzijn en alertheid

Intern aandacht vragen voor nieuwe criminaliteitsrisico's, is zó gedaan. Maar zonder organisatiebreed gevoel van urgentie en betrokkenheid, blijft het beoogde effect vaak uit. Voor bestuurders van verzekeraars ligt hier een cruciale rol Zij moeten medewerkers daadwerkelijk alert en in een 'actiestand' zien te krijgen en houden. Compliance-argumenten resulteren op de werkvloer niet automatisch in intrinsieke motivatie.

Vanuit de bestuurskamer moet concreet worden gemaakt hoe medewerkers in hun werk – en daarbij óók persoonlijk – door frauduleuze en malafide activiteiten geraakt kunnen worden.

Online communicatiemogelijkheden met medewerkers van bedrijven zijn zelden zo aantrekkelijk geweest voor crimineel maatwerk. Iedereen die bij een verzekeraar werkt, moet zich realiseren dat hij op elk moment te maken kan krijgen met geraffineerde pogingen van kwaadwillenden om via individueel mail-, app-, of belverkeer fraude te plegen of onrechtmatig toegang tot systemen of data te krijgen. Social engineering en spearphising nemen steeds geavanceerdere verschijningsvormen aan. [2]

Organisaties en medewerkers moeten zich bewust zijn van hun kwetsbaarheid doordat zakelijke en persoonlijke informatie eenvoudig op het internet is te vinden. Wie denkt hiervoor immuun te zijn, vergist zich. Als gevolg van datadiefstallen en -lekkages is tegenwoordig van vrijwel elke Nederlander informatie op het darkweb beschikbaar.

Verzekeringsfraudeurs mogen zich de komende jaren 'verheugen' in ongekende mogelijkheden om facturen, afbeeldingen en andere documenten met behulp van generatieve AI-tools te vervalsen en te manipuleren. Technische oplossingen in Straight Through Processing (STP) kunnen bij detectie van dergelijke documenten ondersteunen.

Het menselijke 'niet-pluis-gevoel' is echter niet zomaar door technische middelen te vervangen. Het blijft belangrijk dat medewerkers op acceptatie-, schade- of klantcontact-afdelingen zélf over kennis en vaardigheden beschikken om manipulatie te herkennen en om een redelijke eerste beoordeling van onderzoekwaardige signalen te maken.

" Expect the unexpected and be prepared for it "

Een medewerker van een buitenlandse financiële instelling rook recent onraad bij het ontvangen van een verzoek van zijn CFO om in het geheim 25 miljoen dollar over te maken. Als hij hier niet op ingaat wordt hij plots in een videocall 'op het matje geroepen'. Daarin zijn de CFO én zijn voltallige staf schijnbaar aanwezig. De medewerker schrikt hier zo van dat hij het bedrag alsnog overmaakt. Achteraf blijkt de videocall een deepfake-creatie van fraudeurs – nog niet eens zó geavanceerd.

Het fenomeen van 'deepfake-impersonisatie' vraagt de komende tijd in het bijzonder om aandacht. Dit wordt door experts als één van de grootste opkomende digitale criminaliteitsrisico's gezien. Kwaadwillenden doen zich bij deze geavanceerde vorm van identiteitsfraude – via door AI-gecreëerde tekst, audio of video – op overtuigende wijze voor als een bekende of een collega.

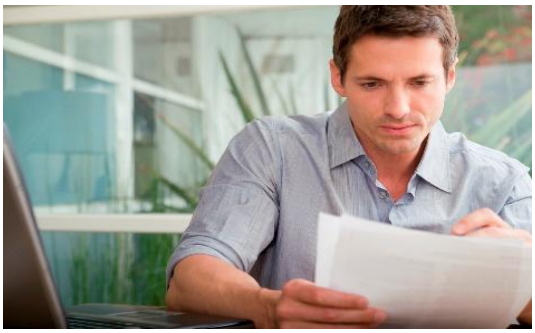
- ➔ Verzekeraars zorgen ervoor dat medewerkers weten hoe zij te maken kunnen krijgen met verschillende vormen van fraude en (cyber)criminaliteit en hoe zij in zulke gevallen daadkrachtig kunnen handelen.
- ➔ Verzekeraars zorgen ervoor dat medewerkers op de hoogte zijn van de nieuwste risico's en criminele modus operandi en over de vaardigheden beschikken om geraffineerde vormen van digitale fraude en manipulatie door kwaadwillenden te herkennen.

- ➔ Het CBV intensiveert en versnelt het uitgeven van marktwaarschuwingen over nieuwe en opvallende vormen van fraude en (cyber)criminaliteit waarmee verzekeraars in aanraking zijn gekomen, - zowel via het Fraudeloket als het i-CERT.
- ➔ Het Verbond faciliteert via o.a. bijeenkomsten en ledencommunicatie dat medewerkers van verzekeraars handvatten krijgen om de meest recente en meest geavanceerde vormen van fraude en criminaliteit effectief te kunnen herkennen en tegen te houden.

[2] *Social engineering* omvat alle manipulatieve technieken die criminelen inzetten om medewerkers er toe te bewegen vertrouwelijke (bedrijfs)gegevens prijs te geven. *Spearphishing* is een vorm van phishing die zich richt op specifieke personen of organisaties om toegang te krijgen tot gevoelige informatie of om malware te installeren.

3. Betrouwbaar met mensen, data en technologie

Consumenten begrijpen het nut en de noodzaak van criminaliteitsbeheersing door verzekeraars. Zij verwachten immers een verantwoorde omgang met hun premiegeld en (klant)gegevens. Maar om risico's goed in te kunnen schatten en buiten de deur te houden, moeten verzekeraars diezelfde (klant)gegevens optimaal kunnen gebruiken. Dit is een wankel evenwicht. Draagvlak voor criminaliteitsbeheersing staat of valt met het hanteren van de hoogste zorgvuldigheidsnormen in de aanpak, transparantie en uitlegbaarheid van processen en besluitvorming.



Voor (aspirant) klanten moet duidelijk zijn waarom zij in aanvraag- en claimprocessen bepaalde vragen krijgen en gegevens moeten aanleveren. Onduidelijke communicatie vanuit de verzekeraar verhoogt het risico op onvolledige of onjuiste informatieverstrekking. Daardoor neemt bijvoorbeeld de kans toe dat mensen onterecht onderwerp van fraudeonderzoek worden. Verzekeraars moeten zich bewust zijn van culturele (communicatie)verschillen en het feit dat verzekeringskwesties voor mensen ingewikkeld kunnen zijn. In het STP-tijdperk moeten zij laagdrempelige mogelijkheden voor individueel contact en uitleg blijven bieden.

- ➔ Verzekeraars leggen in begrijpelijke taal uit welke activiteiten zij ondernemen om de veiligheid en integriteit van hun bedrijfsvoering te beschermen - én op welke punten deze activiteiten concreet aan de belangen van de klant (kunnen) raken.
- ➔ Verzekeraars houden bij het beoordelen van informatie die door consumenten is verstrekt rekening met communicatieverschillen én bieden gelegenheid om onbedoeld onjuiste informatie te corrigeren.
- ➔ Verzekeraars bieden contactmogelijkheden om processen in het kader van risico- en criminaliteitsbeheersing 'op maat' toe te lichten.

- ➔ Het Verbond gaat werken aan een herkenbare, en voor een breed publiek toegankelijke, online vindplaats met informatie en consumentenvoorlichting over de activiteiten van verzekeraars rond de aanpak van fraude en (cyber)criminaliteit.
- ➔ Het Verbond richt voor verzekeraars een kennisbank in met good practices rond het toepassen van de 'menselijke maat' op het terrein van fraude- en criminaliteitsbeheersing.
- ➔ Het Verbond acteert proactief ter voorkoming van ongewenste praktijken bij activiteiten in het kader van de aanpak van fraude en (cyber)criminaliteit.

Om signalen die wijzen op onrechtmatigheden te onderscheiden van ruis in gedigitaliseerde processen en een complexe IT-omgeving, kunnen verzekeraars niet om de inzet van nieuwe technologieën heen. Er komen steeds meer hulpmiddelen beschikbaar die (al dan niet door AI) vervalste documenten en afwijkende patronen in omvangrijke datasets en netwerken kunnen herkennen. Intelligente computersystemen doen in seconden wat anders een enorme capaciteitsinzet zou vragen. Het gebruik van objectieve datamodellen en systemen kan eraan bijdragen dat onbewuste menselijke voordoordelen wegblijven uit het proces van fraudedetectie.

Om een efficiencyslag te maken bij arbeidsintensief (nader) onderzoek naar individuele incidenten, loont het voor verzekeraars om concreet met AI aan de slag te gaan. Met gezond verstand en professioneel inzicht kunnen Chat-GPT-achtige toepassingen verantwoord worden benut voor het samenvatten van gespreksverslagen en onderzoeksresultaten en het creëren van tijdlijnen.

Inzet van kunstmatige intelligentie bij criminaliteitsbeheersing mag in geen geval leiden tot volledig geautomatiseerde besluitvorming over het instellen van onderzoeken of maatregelen gericht op personen. Naast bijvoorbeeld een registratie in een waarschuwingsregister kan bij het laatste ook worden gedacht aan het afwijzen van een polisaanvraag of een claim op grond van een fraudeverdenking. Gezien de mogelijke impact op betrokkenen blijft een menselijke beoordeling van de feiten en (persoonlijke) omstandigheden bij dit soort besluitvorming een belangrijke waarborg. De verzekeraar moet besluiten achteraf kunnen toelichten.

Van diverse medewerkers binnen verzekeringsorganisaties vraagt dit om de nodige vaardigheden en kennis. Investeren daarin is noodzakelijk om bij te blijven met de ontwikkelingen. Beter nog is het om, waar mogelijk, op de ontwikkelingen vóór te sorteren. Op het maatschappelijk actuele thema van 'de menselijke maat' rond criminaliteitsbeheersing kan de sector zich bij uitstek in positieve zin onderscheiden.

- ➔ Verzekeraars benutten optimaal de mogelijkheden die intelligente computersystemen in de strijd tegen criminaliteit bieden, maar laten beoordeling van feiten en besluitvorming met een mogelijke negatieve impact op mensen over aan gekwalificeerde medewerkers.
- ➔ Verzekeraars stellen hoge eisen aan onderzoek naar en maatregelen tegen personen en maken bij elk besluit een zorgvuldige en gedocumenteerde afweging tussen het gerechtvaardigd belang en de mogelijke impact op betrokkene(n).

- ➔ Het Verbond organiseert, samen met expertpartners, periodieke kennissessies voor verzekeraars over de kansen van, en praktische mogelijkheden, om kunstmatige intelligentie op een verantwoorde wijze in te zetten in de strijd tegen fraude en (cyber)criminaliteit.
- ➔ Het Verbond onderzoekt - mede in het licht van de risico's en snelle ontwikkelingen rond digitale criminaliteit en kunstmatige intelligentie - op welke punten het bestaande normenkader voor de sector ten aanzien van fraude- en criminaliteitsbeheersing moet worden gemoderniseerd.

4. Optreden tegen criminaliteitsrisico's en ondermijning in de samenleving en de keten

Als één verzekeraar met vakkundig crimineel gedrag in aanraking komt, is de kans groot dat hij niet de enige is. Het CBV signaleert dat fraudeurs, cybercriminelen en malafide netwerken zich vaker met vergelijkbare modus operandi bij meerdere verzekeraars en ketenpartijen tegelijkertijd manifesteren. Beroepsmatige criminaliteit die extern floreert, leidt tot steeds grotere risico's en schadeposten voor de sector zélf. Dikwijls gaat het om bendes die zich stevig in de buitenwereld hebben genesteld en er diverse andere schadelijke en ondermijnende (ook landsgrensoverschrijdende) praktijken op nahouden. Soms wordt zulke criminaliteit onbewust en onbedoeld door de sector gefaciliteerd.

Voor verzekeraars groeit met deze trend het eigen belang, maar ook de maatschappelijke verantwoordelijkheid, om gezamenlijk op te treden tegen criminaliteitsrisico's die zich in de samenleving of de keten voordoen. Meer informatie-uitwisseling op operationeel niveau is nodig om relevante

fenomenen nog sneller te signaleren.[3] Vrijwel elke hieruit voortkomende waarschuwing op sectorniveau leidt tot een waardevolle feedbackcyclus; het fundament om belanghebbende partijen bijeen te kunnen brengen en gecoördineerde acties op te zetten.

De grootste uitdaging die verzekeraars de komende jaren moeten aangaan, is om vanuit operationele krachtenbundeling binnen de sector nóg vaker de stap te maken naar het daadwérkelijk (helpen) wegnemen van een extern criminaliteitsrisico. Meer bereidheid en ruimte om samen te werken met stakeholders of bevoegde instanties is hiervoor vereist. Dit levert niet zómaar resultaten op. Verzekeraars moeten bereid zijn om zich voor langere termijn te committeren aan relevante samenwerkingsverbanden en daarin te geven én te nemen.

Signaalfunctie verzekeraars

Fraudeonderzoekers of cybersecurity specialisten van verzekeraars vangen voortdurend signalen op van externe criminaliteit. Zij stuiten bijvoorbeeld op mobiele bendes die kortlopende autoverzekeringen afsluiten om onder de radar te blijven, gestolen persoonsgegevens die op internet te koop worden aangeboden, henneptelers die hun activiteiten mogelijk maken door hun panden te verzekeren, witwaspraktijken of potentiële terroristen en criminelen die zich willen verzekeren in voorbereiding op een uitreis, aanslag of liquidatie.

Incidenten in de sector die verband houden met georganiseerde criminaliteit, mogen bij opsporingsdiensten en justitie niet buiten beeld blijven. Vanuit het besef dat sommige dadergroepen alléén met repressieve instrumenten effectief kunnen worden bestreden, moeten verzekeraars weer vaker bereid zijn om aangifte te doen. Niet alleen vanuit het directe bedrijfsbelang maar ook voor de belangen van de sector als geheel.

Gegevens vanuit claim- acceptatie en incidentonderzoeksprocessen kunnen van grote waarde zijn bij opsporing en vervolging. Andersom kunnen verzekeraars criminelen financieel treffen door schade langs civielrechtelijke weg of binnen de strafvorderlijke procedure te verhalen. Om een informatie- en verhaalspositie te verkrijgen, is aangifte doen een belangrijke eerste stap.

- ➔ Verzekeraars wisselen op operationeel casusniveau onderling informatie uit om sector-relevante incidenten en criminaliteitsrisico's nóg sneller te signaleren en daar gezamenlijk tegen op te treden.
- ➔ Verzekeraars doen aangifte als zij slachtoffer worden van criminele activiteiten met een georganiseerde achtergrond.
- ➔ Verzekeraars werken actief samen met partijen in de keten en de samenleving om gesignaleerde criminaliteitsrisico's weg te nemen.

- ➔ Het Verbond biedt verzekeraars extra handvatten en tools waardoor zij de mogelijkheden die er zijn voor operationele informatie-uitwisseling op casusniveau nóg beter kunnen benutten en draagt bij aan een actieve lobby vanuit het bedrijfsleven om de wettelijke mogelijkheden hiervoor te verruimen.
- ➔ Het Verbond werkt aan nieuwe landelijke beleidsafspraken met politie en Openbaar Ministerie over de gezamenlijke aanpak van fraude en criminaliteit – en de inzet van het strafrecht daarbij in het bijzonder.
- ➔ Het CBV werkt aan een landelijk netwerk van schakel- en belangenorganisaties in de keten en de samenleving waardoor verzekeraars, bij signalering van externe criminaliteitsrisico's, snel in contact kunnen komen met relevante partijen.

[3] Het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI) en het convenant Computer Emergency Response Team (i-CERT) bieden uitgebreide mogelijkheden om binnen wettelijke kaders invulling te geven aan deze informatie-uitwisseling.

5. Effectief en efficiënt: gezamenlijk oplossingen zoeken

De razendsnelle ontwikkelingen in het dreigingslandschap en de regelgeving, vragen van iedere verzekeraar investeringen om interne maatregelen en structuren rond fraude- en criminaliteitsbeheersing en cybersecurity te versterken. Afgezet tegen de schade die zo wordt voorkomen, verdient elke hieraan besteedde euro zich vrijwel zeker terug. Het lijkt er echter op dat de uitgaven, die noodzakelijk zijn voor het ontwikkelen en implementeren van beheersmaatregelen, ook de komende jaren zullen blijven toenemen. Extra uitdaging is dat verzekeraars bij dit alles in toenemende mate schaarse, specialistische vakkennis en (digitale) expertise nodig hebben.

Tegen deze achtergrond neemt in de sector ook het besef toe dat "ieder voor zich het wiel uitvinden" bij het beheersen van criminaliteitsricio's lang niet altijd tot de uitkomst leidt die het meest doeltreffend is.

Zowel om de stijgende kosten in de hand te houden als om de meest effectieve maatregelen te identificeren, moeten verzekeraars gezamenlijk naar oplossingen op zoek. Versnippering van kennis, succesvolle werkwijzen en initiatieven binnen de sector werken nu nog in het voordeel van de crimineel. Om het tij te keren hebben verzekeraars regie en ondersteuning vanuit het Verbond nodig.

Vooral op operationeel niveau liggen kansen voor verzekeraars om samen te werken, kennis over oplossingen te delen en inkoopkracht te organiseren voor het oprapen. Waar dit voor individuele verzekeraars onhaalbaar of te kostbaar is, kunnen gezamenlijke trainingen vanwege hun schaalgrootte bijvoorbeeld een uitkomst bieden om alsnog specifieke technische vaardigheden rond cybersecurity of fraudebeheersing op te doen.

Het op gang brengen van noodzakelijk onderzoek naar innovatieve maatregelen en interventies, vraagt vrijwel altijd om een collectieve benadering, De ontwikkeling van het Verbond naar een 'open platform' brengt nieuwe mogelijkheden met zich mee om bij gezaghebbende partnerorganisaties waardevolle actuele kennis voor de hele sector te ontsluiten (bijvoorbeeld op het vlak van duiding van jurisprudentie en cybersecurity 'threat intelligence').

- ➔ Verzekeraars werken samen met deskundige partijen buiten de sector om in co-creatie tot nieuwe initiatieven en oplossingen voor criminaliteitsbeheersing te komen.
- ➔ Verzekeraars dragen actief bij aan sectorale kennisdeling over effectieve en efficiënte maatregelen op het terrein van criminaliteitsbeheersing en cybersecurity.

- ➔ Het Verbond stimuleert - en draagt met de centraal bij het CBV beschikbare expertise actief bij aan – onderzoeken naar innovatieve oplossingen op het terrein van criminaliteitsbeheersing die door verzekeraars benut kunnen worden.
- ➔ Het Verbond jaagt het ontstaan van 'fusion centers' aan, waarin experts vanuit uiteenlopende relevante vakgebieden en organisaties - zowel binnen als buiten de sector- de krachten bundelen om oplossingen tegen hardnekkige criminaliteitsproblemen te ontwikkelen.
- ➔ Het Verbond faciliteert samenwerkingsinitiatieven waar deze kunnen bijdragen om medewerkers in de sector toegang te geven tot noodzakelijke training, specialistische kennis en schaarse (digitale) expertise.