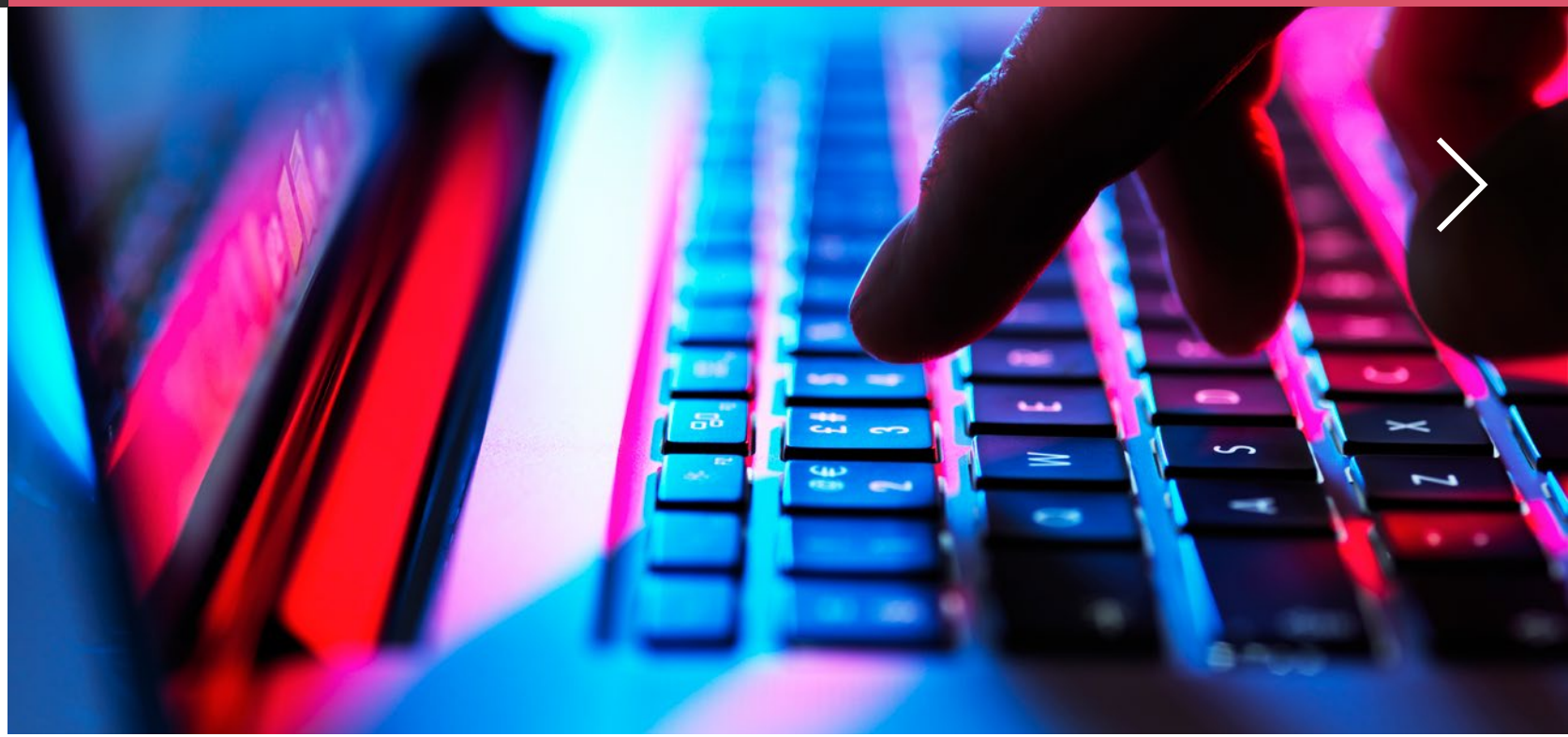
June 2021

Economic Crime Survey Nederland 2021

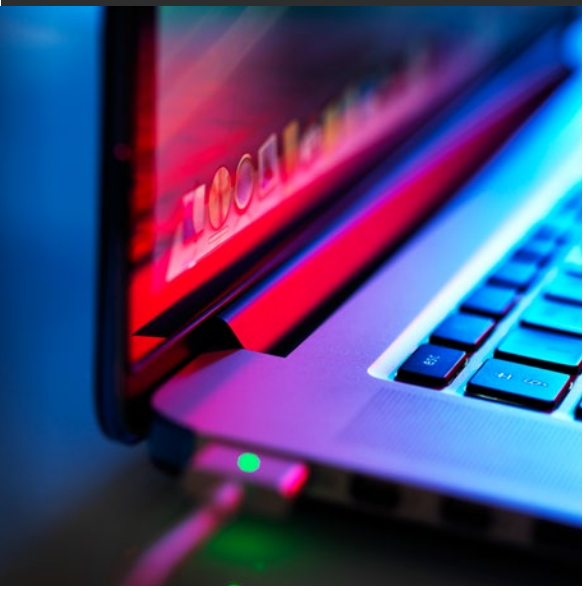
In samenwerking met:

VU VRIJE UNIVERSITEIT AMSTERDAM



pwc

www.pwc.nl



Inhoudsopgave

Sommige browsers ondersteunen niet alle links in de pdf. Download voor de beste gebruikerservaring de pdf en open deze in uw Adobe Acrobat Reader. (https://get.adobe.com/reader/).

Managementsamenvatting

PwC Economic Crime Survey 2021

Op het eerste gezicht schetst deze tiende editie van het onderzoek door PwC Nederland en de sectie Criminologie van de Vrije Universiteit Amsterdam naar de ontwikkeling van financieel-economische criminaliteit in Nederland een geruststellend beeld. Er wordt een daling gerapporteerd van het aantal geconstateerde incidenten. En dat terwijl we door de pandemiedreiging massaal thuiswerken, waarvan altijd is aangenomen dat het de kwetsbaarheid voor de onderzochte criminaliteitsvormen vergroot.

Ondanks werken op afstand toch een daling van financieel-economische criminaliteit, maar…

76% van de respondenten in de Economic Crime Survey 2021 geeft aan dat hun organisatie in de voorbije 24 maanden is geconfronteerd met een of meer 'traditionele' vormen van financieel-economische criminaliteit, zoals diefstal van geld, goederen of fraude, diefstal van informatie, concurrentievervalsende acties of corruptie. Dat is een daling van 7% ten opzichte van 2019.

56% zegt dat zijn of haar organisatie slachtoffer is geweest van cybercriminaliteit. Dat is 4% minder.

Ik voelde opluchting toen ik deze eerste resultaten las. Maar is dat wel terecht?

Onwetendheid verdubbeld

Als we enkele andere waarnemingen uit het onderzoek meewegen, blijkt de situatie in werkelijkheid toch iets minder rooskleurig te zijn.

Zo is het aantal respondenten verdubbeld dat zegt niet of niet zeker te weten of hun organisatie in de afgelopen twee jaar slachtoffer is geweest van diefstal van geld of goederen of fraude – van 9% in 2019 naar 18% nu. De toegenomen onwetendheid verklaart mogelijk een deel van de geconstateerde daling. En uit de kwalitatieve interviews blijkt dat ook de aangifte- en meldingsbereidheid afneemt en men liever eerst zelf onderzoek doet of laat doen. Bovendien zeggen veel organisaties hun financiële prioriteiten te hebben moeten herschikken, wat ten koste gaat van geplande investeringen in betere preventie en detectie. De kwetsbaarheid wordt daardoor groter en de weerbaarheid neemt af.

Wie vreesde dat de sinds 2017 geconstateerde sterke toename van financieel-economische criminaliteit een extra impuls zou krijgen door de gevolgen van de coronacrisis, kunnen we op grond van onze onderzoeksresultaten geruststellen. Maar duidelijk is ook dat veel lange termijneffecten zich nog vooral onderhuids manifesteren. Ik reken me daarom tot de experts die verwachten dat de 'grote klap' wellicht komt als we weer terug naar normaal gaan. Wel kan worden geconstateerd dat de stijgende trend van de laatste jaren zich niet heeft doorgezet – en dat is beter nieuws dan mocht worden verwacht.

Jubileumeditie van unieke indicator

Bovenstaande vaststelling is voor mij de belangrijkste uitkomst van PwC's Economic Crime Survey 2021. Het is de jubileumeditie van een onderzoekreeks, twintig jaar geleden begonnen als Nederlandse bijlage van de Global Economic Crime & Fraud Survey van de internationale organisatie van PwC.

Om een beter inzicht te krijgen in de specifieke eigenschappen en de omvang en ontwikkeling van financieel-economische criminaliteit in Nederland, nam PwC Nederland het initiatief voor een eigen tweejaarlijks onderzoek. Aan de criminologen van de VU werd gevraagd een methodologie en typologie te ontwikkelen die meebeweegt met (en indien mogelijk anticipeert op) de trends waar organisaties, beleidmakers en opsporingsautoriteiten mee geconfronteerd worden of kunnen worden.

Het resultaat is een voor zover mij bekend uniek betrouwbare indicator die zuivere vergelijkingen in de tijd mogelijk maakt en een schat aan data oplevert. Aan de hand van de uitkomsten kan de wetenschappelijke kennis van en over

financieel-economische criminaliteit worden geactualiseerd en de focus van onze forensische onderzoekspraktijk worden bijgestuurd of aangescherpt. Bovendien is het politiek-maatschappelijke debat over dit belangrijke, maar gevoelige onderwerp gebaat bij wetenschappelijk verantwoorde en goed vergelijkbare waarnemingen.

Response van professionals

Ook de resultaten van de 2021-editie mogen weer als representatief worden gepresenteerd. 875 vertegenwoordigers van een evenwichtige dwarsdoorsnede van private en publieke organisaties werkten belangeloos mee, stuk voor stuk professionals die dagelijks bezig zijn met het in kaart brengen, voorkomen of aanpakken van alle denkbare vormen van traditionele financieel-economische criminaliteit en cybercriminaliteit. Daarnaast zijn tien kwalitatieve expertinterviews gehouden om de uitkomsten te toetsen en nader te duiden.

De overige bevindingen van het ECS 2021 vat ik hierbij voor u samen.

Cybercriminaliteit blijft een blinde vlek

- De onwetendheid rond cybercriminaliteit blijft groot. Zoals gemeld geeft 56% (2019: 60%) aan enigerlei vorm van cybercriminaliteit te hebben geconstateerd. Daarmee geeft 44% impliciet toe dit niet of niet zeker te weten. Dat is en blijft een verontrustend grote blinde vlek voor een digitaliserende economie en samenleving.

- Versnippering in cybercriminaliteit. We constateren een nieuwe trend; phishing is met 47% nu de meest gemelde digitale criminaliteitsvorm, gevolgd door malware en hacking. In de laatste twee categorieën constateerden we overigens een aanzienlijke daling, respectievelijk met 15% en 8% ten opzichte van vergelijkingsjaar 2019. DDoS-aanvallen komen minder vaak voor (16%), net als chantage door ransomware (20%) en social engineering (16%). Bij deze uitkomsten moet wel in aanmerking worden genomen dat in de vragenlijsten van de huidige editie voor het eerst deze specifieke cybercriminaliteitsvormen werden voorgelegd, wat versnippering in de hand werkt. Tevens komt uit de interviews met de experts naar voren dat naast ransomware, ook andere vormen van cybercriminaliteit worden ingezet als middel tot afpersing.

Bouwketen probleemsector

- Bouwnijverheid is de zwaarst getroffen sector. Zowel wat traditionele financieel-economische criminaliteit als cybercriminaliteit betreft. Zo komen 5 van de 7 meest geconstateerde cybercriminaliteitsvormen voor in de bouwketen. Gezien de economisch druk op de sector en de maatschappelijke wens om het bouwtempo te verhogen, lees ik dit als een pleidooi voor het afdwingen van meer zekerheden in de sector.

(Nog?) geen brexit-effect

- Het verwachte Brexit-effect blijft uit. Gevraagd of ze een verhoogd frauderisico in het grensoverschrijdend goederenverkeer verwachten doordat het VK de EU heeft verlaten, antwoordt een meerderheid ontkennend. Wel geeft 21% aan meer problemen te vrezen bij de naleving van niet-fiscale maatregelen, zoals het niet voldoen aan de EU-maatregelen op het gebied van gezondheid, milieu of productveiligheid. Onduidelijk is of het frauderisico wordt ontkend of onderschat.

Minder binding door thuiswerken

- Thuiswerken verzwakt de band met de organisatie. 37% van de respondenten zegt minder binding van thuiswerkende medewerkers met hun organisatie te ervaren. 1 op de 5 denkt dat de weerbaarheid van de organisatie is afgenomen (35% vindt van niet) en 31% vreest dat de integriteitsbeoordeling van nieuwe zakelijke contacten in de huidige omstandigheden minder zorgvuldig gebeurt. Weliswaar betreft het nog een minderheid, maar het is wel een volgende indicatie voor een zorgelijk bijeffect van langdurig meer thuiswerken.
- Afname interne tips. Het aantal respondenten dat aangeeft op grond van een interne tip een onderzoek te starten, is teruggelopen van 31% naar 24% nu. Ook dit lijkt te wijzen op een verlies aan betrokkenheid. Daar staat tegenover dat 34% nu beschikt over een meldpunt voor klokkenluiders (was 28%), wat betekent dat de meeste (middel)grote organisaties voldoen aan de vastgelegde wettelijke plicht die eind dit jaar van kracht wordt middels de Wet bescherming klokkenluiders.

Meer zelfonderzoek

- De markt voor zelfonderzoek groeit. De aangiftebereidheid neemt af; 30% zegt aangifte te doen van aan het licht gekomen traditionele criminaliteitsincidenten. De keerzijde is dat 70% liever voor zelfonderzoek kiest of de zaak de zaak laat. Daarvan schakelt 11% een advocaat in en 10% een forensisch accountant. Dit is brandstof voor de discussie over hoe meer zelfonderzoek in goede banen moet worden geleid.

Meer vrouwen

- Meer vrouwelijke daders. De logische keerzijde van het gevoerde emancipatiebeleid in de hogere managementlagen laat zich zien: van de interne daders is 24% (2019: 19%) vrouw. Het interne daderprofiel is overigens nog altijd overwegend mannelijk (67%), gemiddeld 36 jaar oud en meest actief op middenmanagementniveau.

Maar een klein beetje meer compliance

- Compliance in de lift. 29% zegt over een compliance-programma te beschikken, een plus van 3%. Opvallend blijft dat (te) veel van onze respondenten, mannen en vrouwen die toch middenin in de praktijk staan, niet zeker zeggen te weten of hun organisatie aan compliance doet - en dus ook de informatie daarvan niet benutten. Vooral bij kleine en middelgrote organisaties speelt dit. Ook opvallend: maar 63% van de bevraagde financiële instellingen geeft aan te voldoen aan de eind van dit jaar van kracht wordende wettelijke verplichting om een compliance-programma in te richten. Ook als een voorbehoud wordt gemaakt voor uitzonderingen voor wie deze plicht niet geldt, verdient dit nader onderzoek.

En te weinig data-analyse

- Data-analyse is een nog altijd onderbenut preventie- en detectie-instrument. Weliswaar geeft 28% (plus 3%) aan de mogelijkheden van data-analyse te benutten, maar gezien de digitale en traditionele bedreigingen is dat nog altijd een verontrustend laag cijfer. 39% geeft onomwonden toe ook geen plannen te hebben.

Al met al denk ik met u te mogen constateren dat deze editie van het Economic Crime Survey 2021 weer een rijke oogst aan nieuwe inzichten, verduidelijkingen en waarschuwingen oplevert. Genoeg om ons te helpen de complexe bedreiging door financieel-economische criminaliteit beter het hoofd te kunnen bieden. Uiteraard zijn wij, van de forensische onderzoekspraktijk van PwC, graag bereid u daarbij terzijde staan.

Tot slot bedank ik het onderzoeksteam, in het bijzonder Sebastiaan van Zijl die, in samenwerking met twee stagiaires Job Jebbink en Reggie Hoost, namens PwC het onderzoek coördineerde, en Wim Huisman en Clarissa Meerts van de VU voor hun wetenschappelijke inbreng.

Amsterdam, 17 juni 2021

Andreas Mikkers
Partner Forensic Services

1. Prevalentie van traditionele financieel-economische criminaliteit

In de PwC Economic Crime Survey 2021 zijn 875 respondenten geselecteerd en geënquêteerd die binnen bedrijven en andere organisaties belast zijn met het in kaart brengen, voorkomen of aanpakken van financieel-economische criminaliteit. De bevindingen zijn vervolgens in interviews voorgelegd aan 10 experts uit de publieke en private sector. In dit onderzoek wordt gekeken naar financieel economische criminaliteit, wat als overkoepelende term wordt gebruikt voor traditionele financieel-economische criminaliteit en cybercriminaliteit.

Financieel-economische criminaliteit kan worden gedefinieerd als het misleidende of onrechtmatig gebruik van een op geld waardeerbaar aspect binnen of in relatie tot een zakelijke aangelegenheid (Faber, 2011).
Onder traditionele financieel-economische criminaliteit worden vormen van criminaliteit met een financieel-economisch oogmerk verstaan die ook voor de komst van computers en het internet konden worden gepleegd. Hoofdvormen zijn diefstal van geld of goederen of fraude, corruptie, diefstal van informatie en concurrentievervalsing. Desalniettemin zullen deze vormen van criminaliteit tegenwoordig vooral met digitale middelen worden gepleegd. Onder cybercriminaliteit verstaan we vormen van criminaliteit waarbij IT-systemen doelwit vormen en die alleen met digitale middelen kunnen worden gepleegd.

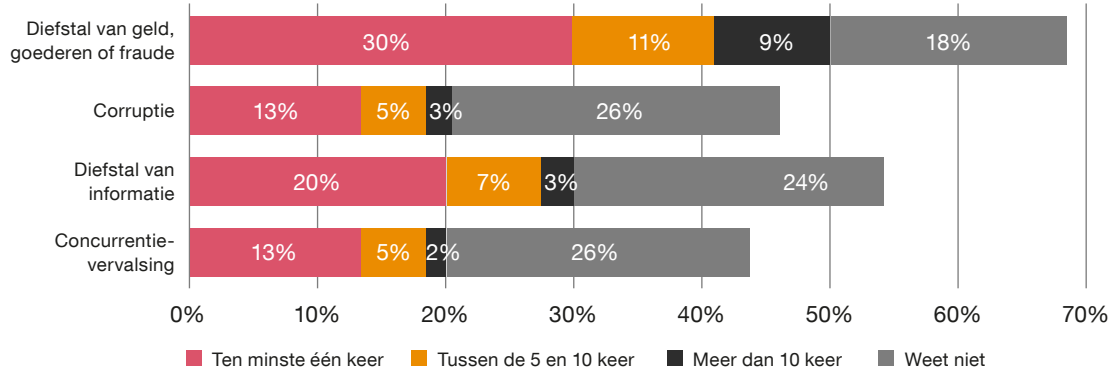
Omvang van financieel-economische criminaliteit

In de vorige editie van de Economic Crime Survey uit 2019 was de prevalentie van financieel-economische criminaliteit gestegen van 73% naar 83%. In deze editie is 76% van de respondenten in aanraking gekomen met een vorm van financieel-economische criminaliteit. In aanraking komen met criminaliteit kan zowel betekenen dat de organisatie slachtoffer is geworden van criminaliteit als dat daders hebben gehandeld in naam van de organisatie. Ondanks een lichte daling ten opzichte van de vorige editie, is nog steeds een algehele stijging van financieel-economische criminaliteit waar te nemen sinds de Economic Crime Survey van 2017.

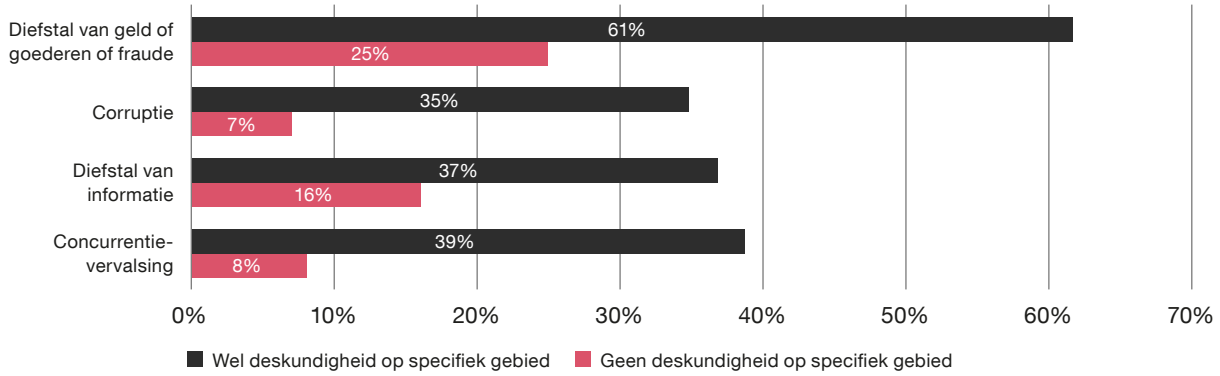
Verschillende vormen van traditionele financieel-economische criminaliteit

In *figuur 1* staan de vier vormen van traditionele financieel-economische criminaliteit centraal, namelijk diefstal van geld

Figuur 1 Prevalentie van traditionele financieel-economische criminaliteit



Figuur 2 Deskundigheid en prevalentie traditionele financieel-economische criminaliteit



of goederen of fraude, corruptie, diefstal van informatie en concurrentievervalsing. 50% van de respondenten geeft aan dat in de afgelopen twee jaar sprake is geweest van diefstal van geld of goederen of fraude. Dit is een daling ten opzichte van 2019, waar diefstal van geld of goederen of fraude nog bij 61% van de respondenten voorkwam. Ook bij corruptie is de prevalentie gedaald van 26% in 2019 naar 21% in 2021. Vervolgens gaf 30% van de respondenten aan slachtoffer te zijn geweest van diefstal van informatie. Dit geeft een daling weer van 10% in vergelijking met de prevalentie van 2019. Wanneer gekeken wordt naar concurrentievervalsing is een daling van 6% zichtbaar. In 2021 komt concurrentievervalsing voor bij 20% van de respondenten. Ten opzichte van de editie uit 2019 rapporteren de respondenten in 2021 dus een algehele daling van traditionele financieel-economische criminaliteit.

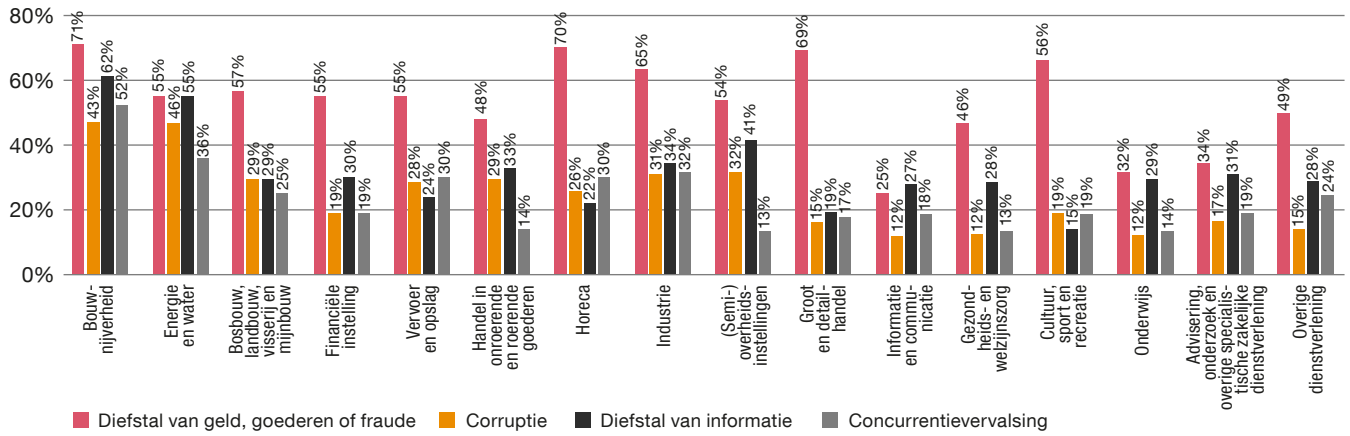
Het is verleidelijk de daling toe te schrijven aan de gevolgen van de coronacrisis van 2020 en 2021. Vanwege de lockdowns en de oproep tot thuiswerken hebben verschillende wetenschappers en politieorganisaties een verschuiving van traditionele criminaliteit naar cybercriminaliteit voorspeld (Huisman, 2021). Op de gevonden prevalentie van cybercriminaliteit gaan we in het volgende hoofdstuk in. Een andere mogelijk verklaring is dat door het thuiswerken minder financieel-economische criminaliteit binnen organisaties is gedetecteerd en door onze respondenten wordt gerapporteerd. Op de samenhang tussen thuiswerken tijdens de coronacrisis en prevalentie van financieel-economische criminaliteit gaan we in hoofdstuk 7 nader in.

Een andere mogelijke verklaring voor de daling van gerapporteerde financieel-economische criminaliteit hangt samen met een verandering in het aandeel respondenten met specifieke deskundigheid op het terrein van de onderzochte vormen van criminaliteit. In *figuur 2* is de prevalentie van traditionele financieel-economische criminaliteit weergegeven die gerapporteerd is door respondenten met en zonder specifieke deskundigheid op de respectievelijke vorm van financieel-economische criminaliteit. Hieruit blijkt dat grote verschillen bestaan tussen rapportage van deskundigen en niet-deskundigen. 39% van de deskundigen meldt bijvoorbeeld een geval van concurrentievervalsing en slechts 8% van de niet-deskundigen. Ook de overige vormen van traditionele financieel-economische criminaliteit leveren soortgelijke verschillen op. Hieruit blijkt het belang van het hebben van deskundigheid voor het meten van de prevalentie van financieel-economische criminaliteit. Om het belang van het hebben van deskundigheid bij het rapporteren van traditionele financieel-economische extra te benadrukken, is een phi correlatie uitgevoerd[1]. Hieruit kan geconcludeerd worden dat onder respondenten met deskundigheid op het gebied van traditionele financieel-economische criminaliteit vaker slachtofferschap wordt gerapporteerd dan onder respondenten zonder deskundigheid.

Een andere opvallende uitkomst is een stijging in het aantal respondenten dat aangeeft niet te weten of hun organisatie slachtoffer is geworden van traditionele financieel-

1 Deze phi correlatie meet samenhang tussen twee dichotome variabelen (bijvoorbeeld met antwoordcategorie ‘ja’ of ‘nee’), waarbij de sterkte van het verband berekend wordt. Hiervoor is een nieuwe variabele aangemaakt die aangeeft of de respondent wel of geen deskundige is op het gebied van traditionele financieel-economische criminaliteit. Vervolgens is voor deze variabele en de variabele prevalentie van traditionele financieel-economische criminaliteit een phi-correlatie uitgedraaid. Daarbij gaat het om een zwak positief verband (0,171).

Figuur 3 Prevalentie van traditionele financieel-economische criminaliteit per sector

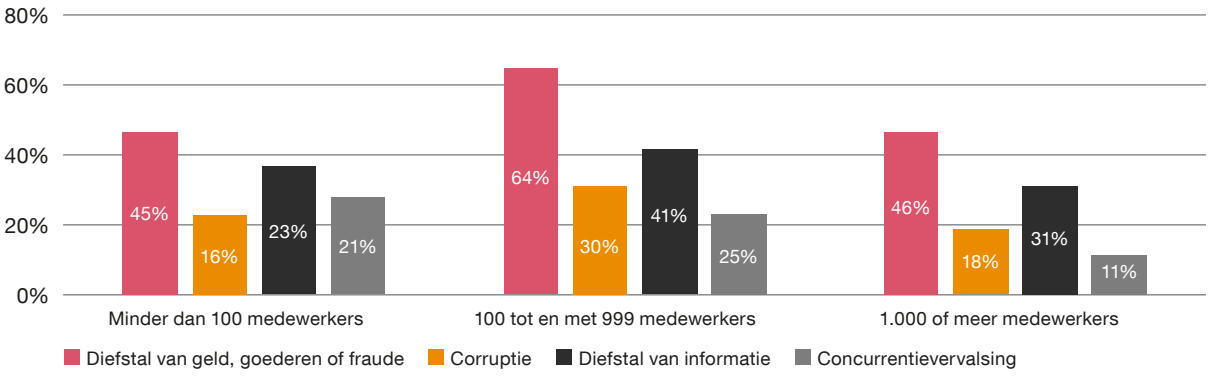


Per organisatie verschilt de financieel-economische criminaliteit

Niet alleen de algemene prevalentie van de verschillende soorten financieel-economische criminaliteit is onderzocht. In *figuur 3* is de prevalentie van traditionele financieel-economische criminaliteit per sector weergegeven, waartoe de organisatie (hoofdzakelijk) behoort. Net als de afgelopen edities is de prevalentie voor diefstal van geld of goederen of fraude en diefstal van informatie in vrijwel alle sectoren het hoogst. In minder sectoren werden bedrijven slachtoffer van concurrentievervalsing en corruptie. In de sector bouwnijverheid liggen de cijfers voor de vier vormen van traditionele financieel-economische criminaliteit relatief het hoogst.

economische criminaliteit. In het geval van diefstal van geld of goederen of fraude is het aantal respondenten dat aangeeft niet te weten of zijn of haar organisatie in aanraking is gekomen met traditionele financieel-economische criminaliteit ten opzichte van 2019 zelfs verdubbeld van 9% naar 18%. Dit verschil sluit aan bij figuur 2 waaruit opgemaakt kan worden dat het aantal deskundigen dat deze vormen van financieel-economische criminaliteit meldt ook gedaald is. Hiermee kan dus ook de daling in figuur 1 verklaard worden. Als deskundigen meer prevalentie rapporteren dan niet-deskundigen en we hebben minder deskundigen in de steekproef, dan kun je dus ook een daling van gerapporteerde criminaliteit verwachten.

Figuur 4 Prevalentie traditionele financieel-economische criminaliteit en aantal medewerkers in Nederland

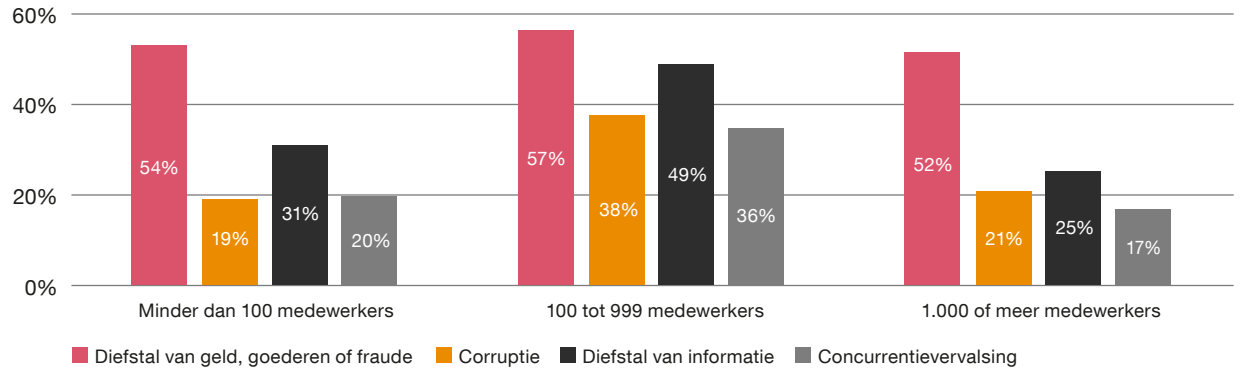


“Waar geld is, vindt je automatisch een goede motivatie voor het plegen van fraude.”

Op basis van dit onderzoek kan geconcludeerd worden dat de meeste slachtoffers van diefstal van geld of goederen of fraude werkzaam zijn in de bouwnijverheid, horeca, industrie of groot- en detailhandel. Dit betreffen sectoren die in hun bedrijfsvoering veel te maken hebben met fysieke goederen. Dit in tegenstelling tot bijvoorbeeld de informatie- en communicatiesector waarbij de prevalentie van diefstal van informatie het hoogst ligt. Wanneer gekeken wordt naar de relatieve prevalentie cijfers valt op te merken dat de informatie en communicatiesector en het onderwijs het minst vaak in aanraking is gekomen met traditionele financieel-economische criminaliteit. Ook geeft een geïnterviewde expert aan dat het per sector kan verschillen hoe duidelijk het is of iets betiteld kan worden als diefstal van geld of goederen of fraude. Bij de ene sector kan het gaan om ‘simpele’ diefstallen, waar andere sectoren te kampen hebben met ingewikkelde fraude casuïstiek. Een voorbeeld wordt gegeven door een expert uit de financiële sector die vertelt: *“Waar geld is, vindt je automatisch een goede motivatie voor het plegen van fraude.”*.

Naast een onderscheid in sectoren, kan ook gekeken worden naar het aantal medewerkers van de organisaties van de respondenten in Nederland. Uit *figuur 4* blijkt dat voor alle vormen van traditionele financieel-economische criminaliteit, het hoogste prevalentiecijfer is gevonden voor de organisaties die 100 tot en met 999 medewerkers in dienst hebben. Lagere prevalentiecijfers worden gevonden voor organisaties met minder dan 100 medewerkers en 1000 of meer medewerkers. Daarbij dient echter wel de kanttekening gemaakt te worden dat nagenoeg 50% van de respondenten werkt bij een organisatie met minder dan 100 medewerkers. De categorieën 100 tot en met 999 medewerkers en 1000 of meer medewerkers zijn elk goed voor om en nabij 25% van de respondenten. Dit verschil in steekproefgrootte kan mogelijk een oorzaak zijn van deze verhoudingen. Deze bevindingen liggen in lijn met de uitkomsten van de Economic Crime Survey 2019. Het grootste verschil is wederom dat de aantallen licht gedaald zijn.

Figuur 5 Prevalentie traditionele financieel-economische criminaliteit en aantal medewerkers wereldwijd

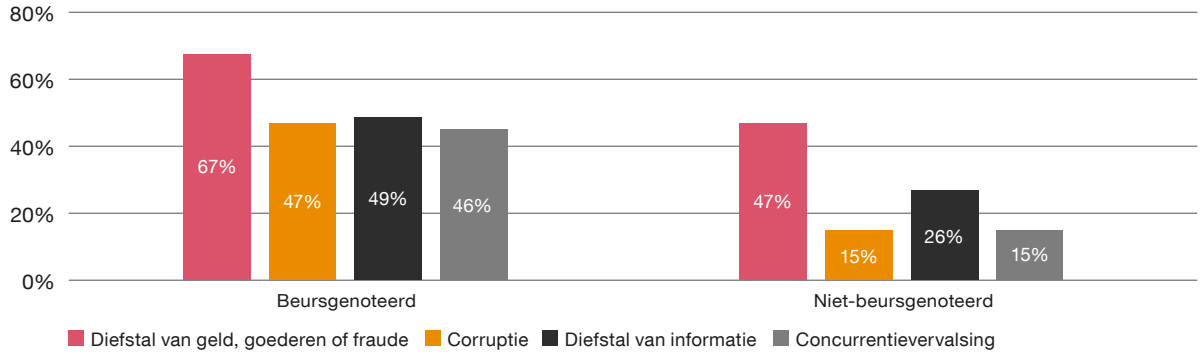


In *figuur 5* is te zien dat organisaties in de categorie van 100 tot 999 werknemers wereldwijd, relatief het vaakst slachtoffer zijn van traditionele financieel-economische criminaliteit. Corruptie, diefstal van informatie en concurrentievervalsing hebben bij organisaties met 100 tot en met 999 medewerkers substantieel hogere prevalentiecijfers ten opzichte van kleine en grote bedrijven.

Daarnaast is ook gevraagd of respondenten werkzaam zijn bij een organisatie die aan een nationale of internationale beurs genoteerd is. Uit onze analyse blijkt dat 16% van de respondenten werkt bij een beursgenoteerd bedrijf en dat 79% bij een niet-beursgenoteerd bedrijf werkt. Uit *figuur 6* blijkt dat beursgenoteerde bedrijven relatief kwetsbaarder zijn voor alle vier de onderzochte varianten van traditionele financieel-economische criminaliteit. Met name corruptie, diefstal van informatie en concurrentievervalsing hebben aanzienlijk hogere relatieve prevalentie. Uit het onderzoek blijkt dat 47% van de beursgenoteerde bedrijven te maken heeft gehad corruptie en ‘slechts’ 15% van de niet beursgenoteerde bedrijven. Deze bevindingen liggen in lijn met de verschillen die gevonden zijn in de editie van 2019.

In de Economic Crime Survey 2019 is voor het eerst gevraagd of organisaties gefinancierd zijn door private equity. Daarom kan dit jaar voor het eerst gekeken worden naar de ontwikkelingen rondom deze investeringsvorm en haar (mogelijke) invloed op financieel-economische criminaliteit.

Figuur 6 Prevalentie traditionele financieel-economische criminaliteit waarbij het moederbedrijf is genoteerd aan een nationale of internationale beurs

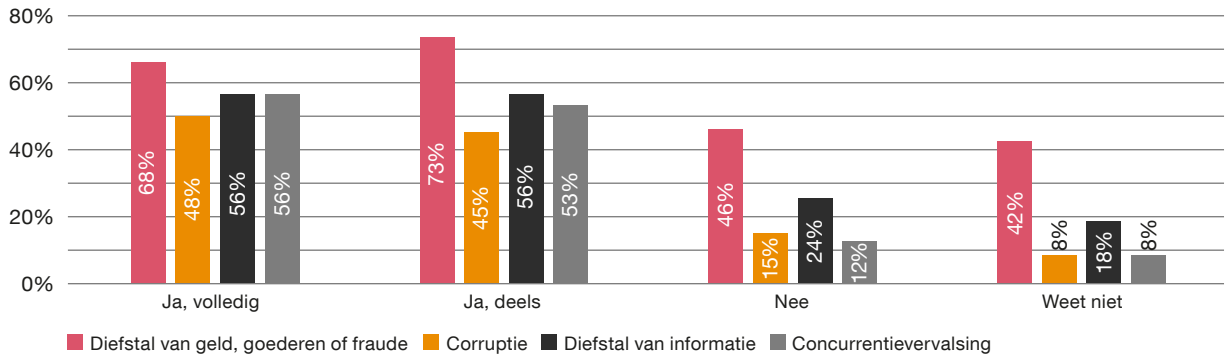


tussen het Verenigd-Koninkrijk en de rest van de wereld teweeggebracht. Om die reden is in deze editie van de Economic Crime Survey gevraagd of de respondenten een verhoogd frauderisico verwachten op het gebied van grensoverschrijdend goederenverkeer naar aanleiding van de Brexit. Uit *figuur 8* valt op te maken dat het grootste deel van de respondenten geen verhoogd frauderisico verwacht naar aanleiding van de Brexit. Desondanks geeft 21% aan een verhoogd frauderisico te verwachten op het gebied van niet-fiscale maatregelen. Deze maatregelen houden in dat goederen niet voldoen aan de EU-normen voor gezondheid, milieu en/of productveiligheid. Respectievelijk 12% en 13% van de respondenten verwacht een verhoogd frauderisico op het gebied van de douanewaarde of de oorsprong. Douanewaarde houdt in dat er te veel of juist te weinig

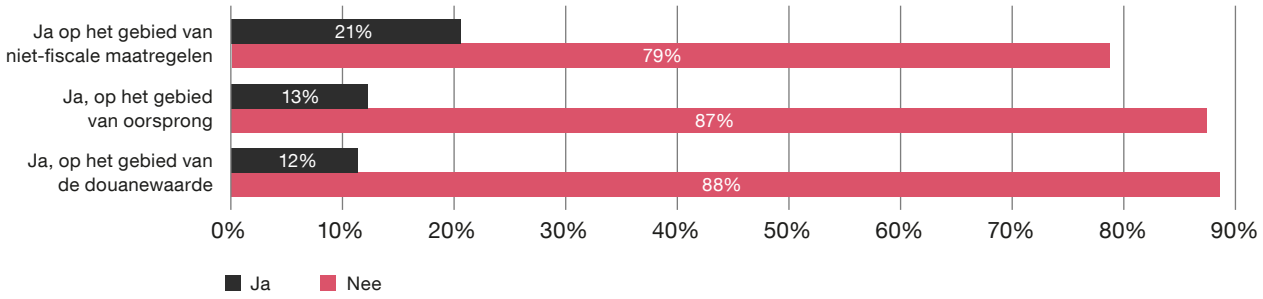
Uit onze analyse blijkt dat 9% van de respondenten aangeeft dat hun organisatie volledig is gefinancierd door private equity. Dit aantal is nagenoeg gelijk aan de gerapporteerde 10% uit 2019. In 2019 gaf 15% van de respondenten aan dat hun organisatie deels gefinancierd is door private equity. In deze editie daalde dat aantal naar 11%. Het beeld dat in 2019 geschetst is, kan door het huidige onderzoek bevestigd worden. Uit *figuur 7* blijkt dat organisaties die (deels) gefinancierd zijn door private equity vatbaarder zijn voor traditionele financieel-economische criminaliteit.

Een onderwerp dat dit jaar aan de Economic Crime Survey is toegevoegd, is de mogelijke invloed van de Brexit op frauderisico's. Het Verenigd-Koninkrijk heeft vier jaar na het referendum de Europese-Unie verlaten. De Brexit heeft niet enkel zijn invloed uitgeoefend op het politieke systeem, maar ook veranderingen omtrent handelsovereenkomsten

Figuur 7 Prevalentie traditionele financieel-economische criminaliteit waarbij de organisatie gefinancierd is door private equity



Figuur 8 Verwacht u voor uw organisatie een verhoogd frauderisico op het gebied van grensoverschrijdend goederenverkeer naar aanleiding van de Brexit?



invoerrechten worden betaald en de oorsprong houdt in dat er ten onrechte verlaagde of geen douanerechten worden toegepast.

Een van de experts geeft in het interview aan dat de Brexit ertoe heeft geleid dat vooral in de financiële sector bedrijven naar Nederland zijn verplaatst. Een mogelijk gevolg hiervan zou kunnen zijn dat door een toename van het aantal organisaties in de sector het voor een toezichthouder moeilijker kan zijn om toezicht te houden.

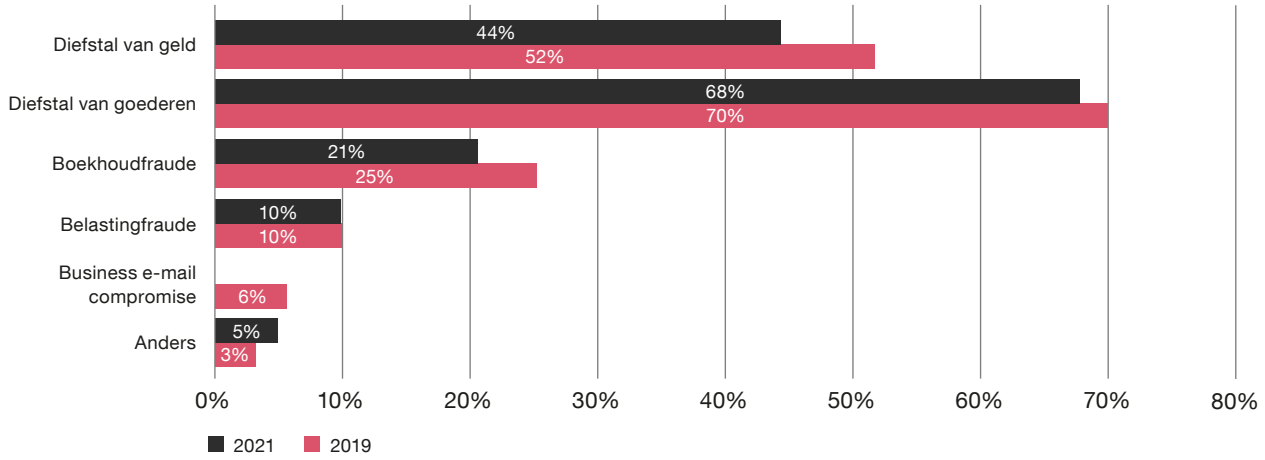
Traditionele financieel-economische criminaliteit onder een vergrootglas

Tot dusver is traditionele financieel-economische criminaliteit enkel opgedeeld in vier hoofdvormen, namelijk diefstal van geld of goederen of fraude, corruptie, diefstal van informatie of concurrentievervalsing. Binnen deze categorieën is naar onderliggende vormen van criminaliteit gevraagd.

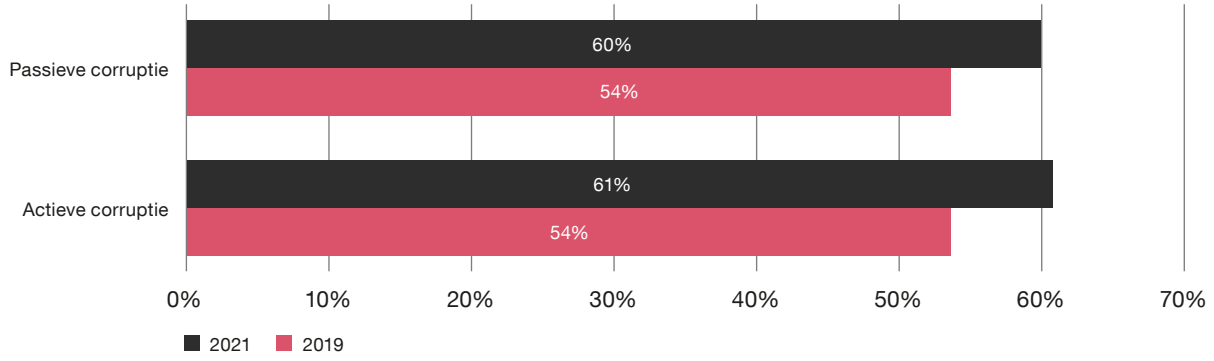
Om te beginnen kan diefstal van geld of goederen of fraude onderverdeeld worden in diefstal van geld, diefstal van goederen, boekhoudfraude en belastingfraude. In *figuur 9* is te zien dat diefstal van goederen en diefstal van geld en boekhoudfraude minimaal zijn afgenomen tot opzichte van de editie uit 2019. Diefstal van geld is het sterkst gedaald van 52% in 2019 naar 44% in 2021. Belastingfraude is daarentegen in prevalentie gelijk gebleven ten opzichte van de vorige editie en de categorie ‘anders’ is licht gestegen met 2%.

Daarnaast kan corruptie onderverdeeld worden in actieve en passieve omkoping. Het aanbieden, geven of beloven van geld, goederen of diensten ter beïnvloeding

Figuur 9 Diefstal van geld of goederen of fraude



Figuur 10 Corruptie

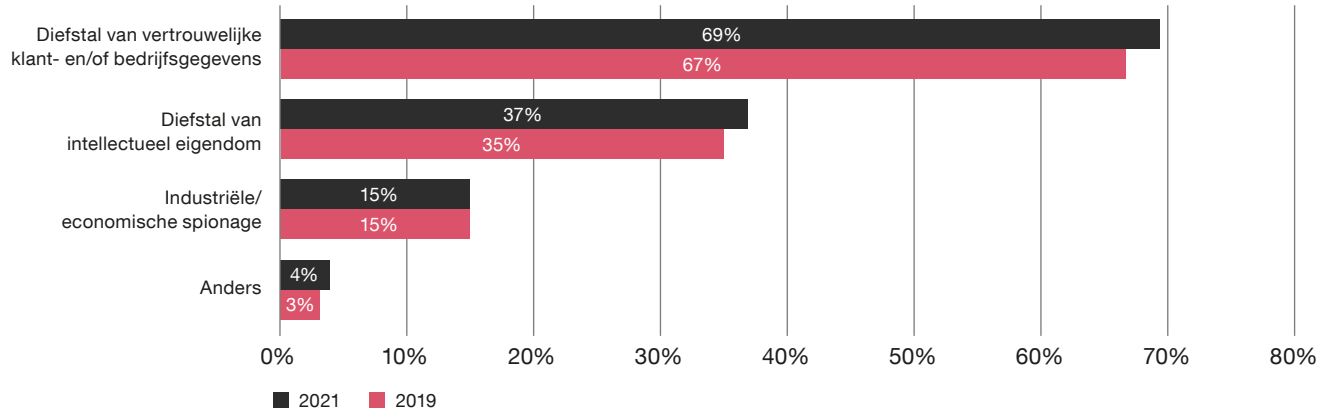


van professionele beslissingen wordt actieve omkoping genoemd. Passieve omkoping houdt in dat individuen geld, goederen of diensten vragen, accepteren of verwachten (Gorsira, Steg, Denkers & Huisman, 2018). Een wisselwerking tussen beide vormen van corruptie is aannemelijk. In *figuur 10* is te zien dat de prevalentie van de twee vormen van corruptie nagenoeg gelijk is gebleven in vergelijking met het onderzoek uit 2019.

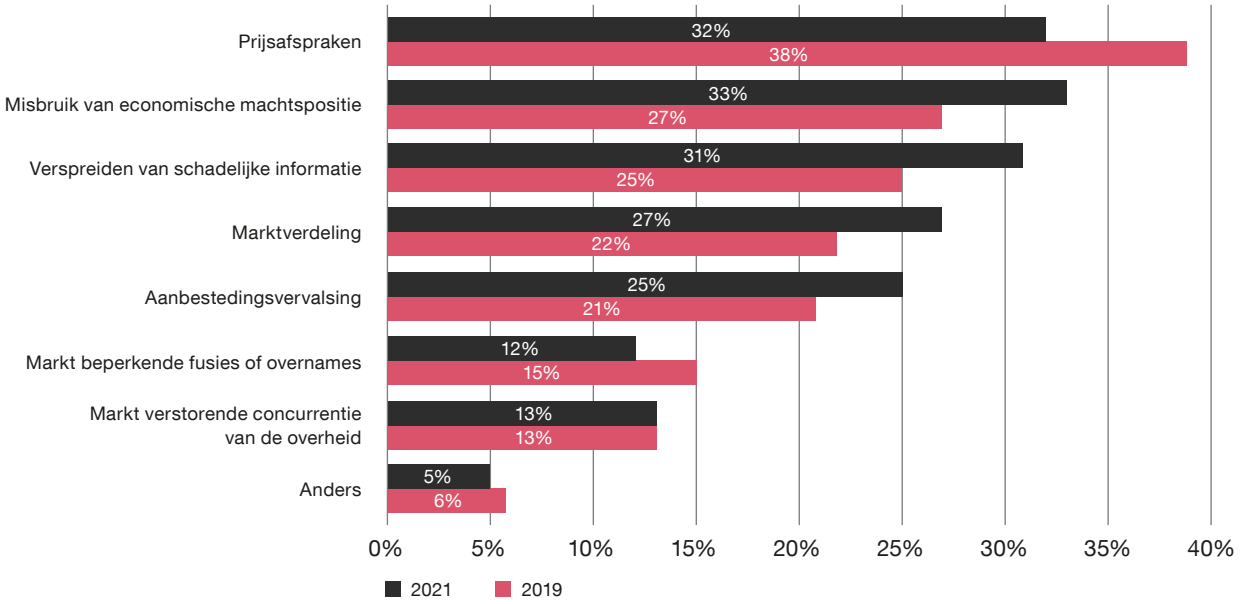
Een expert merkt over corruptie het volgende op:
"In het middenmanagement kan er soms spanning en onvrede ontstaan over bijvoorbeeld het gebrek aan doorgroeimogelijkheden. Dit kan omslaan in cynisme naar de organisatie, wat weer een voedingsbodem is voor bepaald gedrag, bijvoorbeeld corruptie."

Diefstal van informatie is gespecificeerd in drie vormen, namelijk diefstal van vertrouwelijke klant- en/of bedrijfsgegevens, diefstal van intellectueel eigendom en industriële/economische spionage. In *figuur 11* vindt u de prevalentie van de bovenstaande vormen van diefstal van informatie. Hierbij is opmerkelijk dat geen enkele vorm van diefstal van informatie is gedaald. Waar bij overige vormen van traditionele financieel-economische criminaliteit een algehele daling zichtbaar is, is diefstal van informatie grotendeels gelijk gebleven. Bij diefstal van vertrouwelijke klant- en/of bedrijfsgegevens en diefstal van intellectueel eigendom is sprake van een stijging van 2%.

Figuur 11 Diefstal van informatie



Figuur 12 Concurrentievervalsing



Meerdere geïnterviewde experts geven aan een soortgelijke trend te zien voor diefstal van informatie. Waar een daling van diefstal van geld of goederen of fraude logisch wordt geacht, verwachten experts een stijging op het gebied van diefstal van informatie. Meerdere experts geven aan dat diefstal van informatie plaatsvindt bij hun organisaties onder ZZP'ers en andere tijdelijke inhuurkrachten. Een van de experts uit de sector bouwnijverheid vertelt: *"Het percentage van potentiële diefstal van informatie is hoog in de bouwsector omdat er in het aanbestedingstraject veel gebruik gemaakt wordt van inhuurkrachten. Bij grote tenders bestaat deze markt uit zzp'ers die van de ene naar de andere aanbesteding hoppen door zich te laten inhuren door telkens andere bouwbedrijven en hierbij informatie meenemen."* Daarmee liggen de kwantitatieve resultaten in lijn met de bevindingen uit de afgenomen interviews.

De afgelopen twee jaar is 20% van de respondenten in aanraking gekomen met concurrentievervalsing. Deze vorm van traditionele financieel-economische criminaliteit kan onderverdeeld worden in: prijsafspraken, misbruik van economische machtspositie, verspreiden van schadelijke informatie, marktverdeling, aanbestedingsvervalsing, markt beperkende fusies of overnames en 'anders'. Ondanks dat de algemene prevalentie van concurrentievervalsing is gedaald, zijn in de verdere onderverdeling minimale stijgingen te zien. Deze resultaten zijn te vinden in *figuur 12*. Misbruik van machtspositie, verspreiden van schadelijke informatie, marktverdeling en aanbestedingvervalsing zijn gestegen ten opzichte van de vorige editie. Daarnaast is verspreiden van schadelijke informatie een nieuwe toevoeging uit de Economic Crime Survey van 2019. Toentertijd kwam deze vorm van concurrentievervalsing voor bij 25% van de respondenten. In deze editie van de Economic Crime Survey is deze prevalentie gestegen naar 31%. Prijsafspraken en markt beperkende fusies of overnames zijn daarentegen over de afgelopen twee jaar gedaald.

2. Prevalentie van cybercriminaliteit

Uit de Economic Crime Survey van 2019 is gebleken dat de prevalentie van cybercriminaliteit ten opzichte van de jaren daarvoor aanzienlijk was gestegen. Cybercriminaliteit was toen opgedeeld in fysieke cybercriminaliteit, sociale cybercriminaliteit en misbruik. Deze typologie bleek achteraf lastig herkenbaar voor de respondenten en experts. Daarom is er dit jaar voor gekozen meer gangbare termen te gebruiken. Deze nieuwe typologie bestaat uit malware, hacking, DDoS, social engineering, phishing, misbruik en ransomware. Uit de interviews blijkt dat experts deze vormen van cybercriminaliteit beter herkennen. De specifieke vormen van cybercriminaliteit zullen eerst kort gedefinieerd worden. Vervolgens komt de prevalentie per vorm van cybercriminaliteit aan de orde en zal deze waar mogelijk vergeleken worden met de prevalentie van de voorgaande editie van de Economic Crime Survey.

Malware is een verzamelnaam voor verschillende typen kwaadaardige software. Deze kwaadaardige software kan zichzelf verspreiden op andere computers en doet zich vaak voor als een onschuldig lijkend programma. Enkele voorbeelden hiervan zijn virussen en Trojaanse paarden (Van der Wagen, Oerlemans & Weulen Kranenbarg, 2020).

Hacking wordt in het wetboek van strafrecht (WvSr art. 138ab) ook wel 'computervredebreuk' genoemd en is het opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk zoals een laptop. Dit kan op verschillende manieren gedaan worden, zoals door het toegang verschaffen tot een computer of netwerk door middel van een slimme list. Andere voorbeelden zijn het gebruik maken van op internet aangeboden inloggegevens van een account of het gebruik maken van een computer om een wachtwoord te kraken.

Bij een **DDoS-aanval** bezoeken meerdere computers tegelijk een server van een website, waardoor deze server overbelast en dus onbereikbaar wordt.

Bij **social engineering** zorgen daders ervoor dat slachtoffers zelf een bijdrage leveren aan hun slachtofferschap. Daders gebruiken daarbij misleiding, bedrog en overtuigingstechnieken om ervoor te zorgen dat het doelwit gevoelige informatie deelt, waar de daders vervolgens van kunnen profiteren. Een bekend voorbeeld is CEO-fraude waarbij iemand zich voordoet als leidinggevende en vraagt om bepaalde handelingen te verrichten zoals het doen van een betaling. Een expert van de politie merkt in het interview over deze vorm het volgende op: *"Een belangrijke 'let op' voor potentiele slachtoffers is de menselijke kant van social engineering."*.

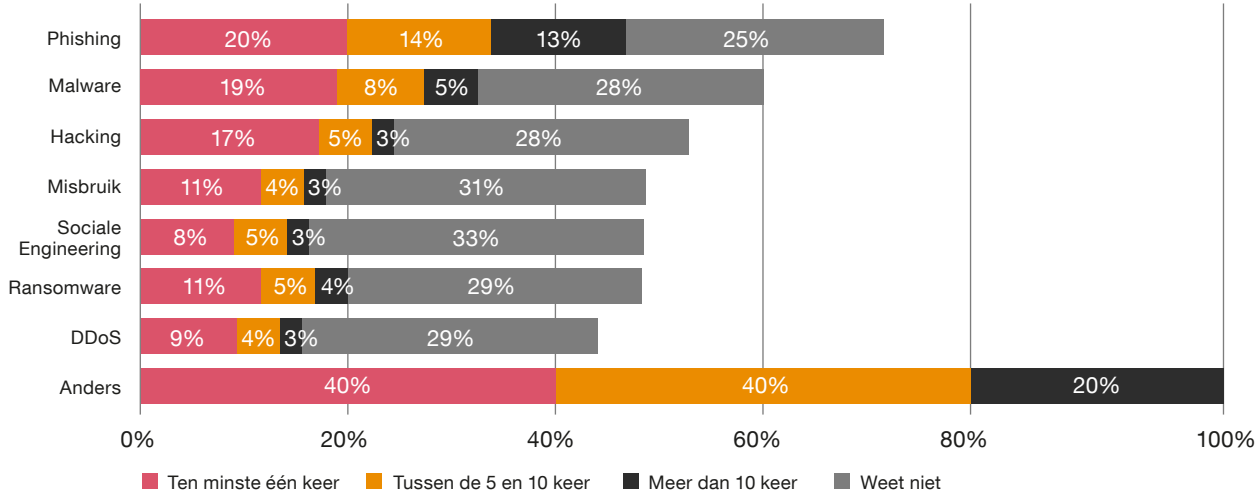
Phishing is een vorm van social engineering, waarbij de dader zich bijvoorbeeld voordoet als een betrouwbare derde partij, zoals een gerenommeerd bedrijf of autoriteit, om op die manier gebruik te maken van gevoelige informatie van het slachtoffer. Dit kan bijvoorbeeld uitgevoerd worden door het slachtoffer een e-mail te sturen, waarin gevraagd wordt naar gegevens of waarbij gerefereerd wordt naar een link. Als vervolgens op de link geklikt wordt, kan de dader achter gevoelige informatie komen zoals persoonsgegevens van het slachtoffer (Bullée, Montoya, Junger & Hartel, 2018).

Misbruik is exclusief voor partijen die een zekere mate van vertrouwen van de organisatie genieten, zoals werknemers en partners. Voorbeelden zijn administratief misbruik, gebruik van beleidsschendingen of het gebruik van niet-goedgekeurde activa.

Ransomware is een vorm van malware die bestanden op afstand kan versleutelen. Vervolgens moet het slachtoffer geld betalen om weer toegang te krijgen tot de bestanden.

Zoals eerder vermeld, is cybercriminaliteit dit jaar op een nieuwe manier bevraagd in vergelijking tot de vorige editie van de Economic Crime Survey. De zeven verschillende vormen van cybercriminaliteit zijn samengevoegd tot een nieuwe variabele. Hierdoor kan de algemene prevalentie van cybercriminaliteit uitgerekend worden. Als een respondent 'ja' invult, dan betekent dit dat de respondent aangeeft slachtoffer te zijn geweest van minstens één vorm van cybercriminaliteit in de afgelopen 2 jaar. Uit analyse blijkt dat 56% van de respondenten uit de vragenlijst slachtoffer is geworden van enige vorm van cybercriminaliteit. Dit is een lichte daling ten opzichte van de vorige editie van de Economic Crime Survey van 2019, toen dit percentage 60%

Figuur 13 Prevalentie van cybercriminaliteit



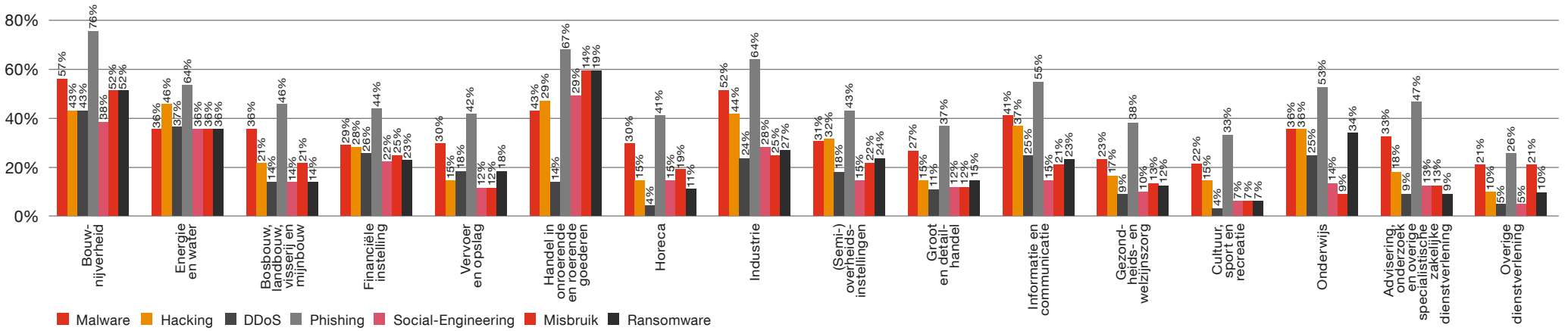
bedroeg. Hierbij dient wel opgemerkt te worden dat dit jaar gebruik is gemaakt van een vernieuwde typologie.

In *figuur 13* is het overzicht van de prevalentie per vorm van cybercriminaliteit te zien. Hieruit blijkt dat phishing, afgezien van de antwoordoptie 'anders', het meest wordt gerapporteerd door de respondenten (47%). Een verklaring hiervoor zou kunnen zijn dat elke individuele medewerker van een organisatie via een email al slachtoffer kan worden van dit type cybercriminaliteit. Daarbij is phishing een relatief makkelijk uit te voeren delict, omdat dezelfde phishingmail naar tal van medewerkers binnen een organisatie kan worden gestuurd. Dat betekent dat daders niet veel moeite hoeven te doen om een groot aantal potentiële slachtoffers te bereiken (Van der Wagen, Oerlemans & Weulen Kranenbarg, 2020).
Daarnaast blijkt uit verschillende interviews met experts dat phishing een veelvoorkomende vorm is van cybercriminaliteit binnen grote organisaties in Nederland. Zo blijkt uit interviews dat organisaties regelmatig testen uitvoeren met werknemers, waarbij werknemers 'namaak' phishingmails opgestuurd krijgen. Een respondent vertelt daarbij dat driekwart van de werknemers tijdens zo een test is ingegaan op de phishingmail. Ook vertelt een van de experts dat phishingmails meer voorkomen in periodes rond de jaarafsluiting waarbij het drukker kan zijn en sneller onbedoeld een verkeerde factuur betaald wordt.

Daarnaast is slachtofferschap van phishing moeilijk tegen te gaan (Leukfeldt, 2014). Zo vertelt een van de experts uit de financiële sector: *"Phishing is ook erg moeilijk te voorkomen omdat het veelal buiten het zicht van banken plaatsvindt, dit terwijl de klant wel van ons vraagt alle vormen van fraude te onderscheppen"*. Daarnaast kan een geslaagde phishingpoging voor veel financiële schade en een lange nasleep zorgen. Daarbij vertelt een andere expert: *"Er hoeft maar één keer iemand op een phishingmail te klikken en het kan een behoorlijk drama geven voor onze ICT-afdeling''*.

Malware wordt vervolgens door 32% van de respondenten gerapporteerd. Dit beeld komt overeen met de resultaten uit de interviews. Zo stelt een van de experts dat malware en phishing binnen zijn organisatie het meest voorkomen. Toch is voor malware een daling van 15% te zien in vergelijking tot de vorige editie van de Economic Crime Survey. Ook bij hacking is een daling te zien ten opzichte van de vorige editie. Dit jaar rapporteert 25% van de respondenten dat zij daar slachtoffer van zijn geworden, terwijl dit 33% was bij de vorige editie. Ditzelfde geldt voor misbruik dat dit jaar door 18% van de respondenten is vermeld. Een mogelijke verklaring voor deze dalingen zou kunnen liggen in het feit dat cybercriminaliteit dit jaar op een (gedeeltelijk) nieuwe manier is uitgevraagd. Zoals eerder vermeld, is dit jaar een andere typologie en zijn meerdere antwoordmogelijkheden gebruikt, waardoor respondenten de kans kregen om slachtofferschap van cybercriminaliteit onder een andere term te scharen. Hierdoor zou een respondent die zijn slachtofferschap in 2019 schaarde onder malware, het dit jaar (ook) zou kunnen classificeren onder bijvoorbeeld ransomware.

Figuur 14 - Prevalentie van cybercriminaliteit per sector



Een mogelijke verklaring voor de afname van de prevalentie van cybercriminaliteit komt naar voren in een van de interviews. Een expert van de politie merkt hierover het volgende op: *"Wij kijken meer op het niveau van volledige datasets, dat is een andere soort telling want wij zien verschillende datasets die op fora meerdere malen worden aangeboden en verrijkt. In jullie data zou het maar één bedrijf zijn die het rapporteert terwijl wij dezelfde dataset meerdere keren zien."*.

De verschillende wetenschappelijke studies naar de ontwikkeling van cybercriminaliteit sinds de uitbraak van de coronacrisis laten verschillende resultaten zien. Verschillen lijken te kunnen worden toegeschreven aan de verschillen in databronnen en meetmethoden die voor deze onderzoeken zijn gebruikt. De studies die een stijging van cybercriminaliteit tijdens de eerste lockdown in de eerste maanden na de uitbraak van de pandemie signaleren, laten vervolgens ook weer een daling in de maanden erna zien (Huisman, 2021).

De vormen die dit jaar het minst vermeld worden zijn ransomware (20%) gevolgd door DDoS (16%) en social engineering (16%). Uit interviews komt naar voren dat ransomware vooral in golven plaatsvindt en het daarom in een bepaalde periode vaker kan voorkomen dan in een andere periode.

Zoals eerder vermeld blijkt uit literatuur dat social engineering in het verlengde ligt van phishing. Een verklaring voor de lage prevalentie social engineering kan daarom liggen in de mogelijkheid dat men slachtofferschap van het delict eerder schaart onder phishing dan onder social engineering.

Naast de totale prevalentie is gekeken hoe de verschillende vormen cybercriminaliteit zijn verdeeld over de sectoren. Uit *figuur 14* blijkt dat malware het meest wordt gerapporteerd door respondenten die werkzaam zijn in de bouwnijverheid (57%). Ook DDoS (43%), phishing (76%), social engineering (38%), misbruik (52%) en ransomware (52%) komen het meest voor in de bouwnijverheid.

“In het onderwijs is er bij ransomware publiciteit voor de gijzelaars, in die zin is het een zichtbaar doelwit”

Opvallend hierbij is dat vijf van de zeven bevraagde vormen van cybercriminaliteit het meest voorkomen in de bouwnijverheid. Dit terwijl respondenten verdeeld zijn over 16 verschillende sectoren. Een mogelijke verklaring hiervoor zou kunnen zijn dat organisaties in de bouwsector zich mogelijk minder bezighouden met preventiemaatregelen tegen cybercriminaliteit. Zo vertelt een expert uit de bouwnijverheid dat de ‘online security’ in zijn organisatie niet gericht is op het voorkomen van cybercriminaliteit maar om zo snel mogelijk weer verder te kunnen gaan, nadat een cyberaanval heeft plaatsgevonden.

Hacking komt het meest voor in de sector energie en water (46%). Wel moet worden opgemerkt dat weinig respondenten uit de survey werkzaam zijn in deze sector waardoor de resultaten voor deze sector minder representatief kunnen zijn. Een expert die werkzaam is in deze sector vertelt dat er minder aandacht is voor financieel-economische criminaliteit in de sector energie en water. Dit kan een mogelijke verklaring zijn voor het lage aantal respondenten uit deze sector. Een andere expert van het OM merkt over de prevalentie in de sector energie en water het volgende op: *“In deze sector wordt veel gebruik gemaakt van oude systemen, als je die stillegt kan je de hoofdprijs vragen omdat het gaat om infrastructuur en kritische processen die gekoppeld zijn aan staatsactoren”.* Tijdens het interview geeft een expert uit de onderwijssector aan dat er in het onderwijs vaker sprake is van malware. Hierover is gezegd: *“In het onderwijs is er bij ransomware publiciteit voor de gijzelaars, in die zin is het een zichtbaar doelwit”*. Een expert van de politie verklaart de relatief hoge prevalentie van DDoS in deze sector met het slachtofferschap van onderwijsinstellingen van cybervandalisme van de eigen studenten.

Verder geeft deze expert aan dat de sector ‘Advisering, onderzoek en overige specialistische zakelijke dienstverlening’ in sommige gevallen het doelwit wordt om de volgende reden: *“Deze bedrijven kunnen interessant zijn in de supply chain en hebben vaak een link aan een bepaalde industrie of grote bedrijven die wel goed beschermd zijn. Wanneer een bedrijf wordt gehacked dat bijvoorbeeld het intranet regelt voor een groter bedrijf kan via een hack van het ene bedrijf ingebroken worden in het ander bedrijf.”*

Een ander opvallend gegeven uit figuur 14 is dat de sector ‘cultuur, sport en recreatie’ op vrijwel alle vormen van cybercriminaliteit de laagste prevalentiecijfers laat zien. Een verklaring hiervoor zou kunnen zijn dat deze sector vooralsnog mogelijk minder digitaal georiënteerd is en dat werkprocessen minder zijn geautomatiseerd. Ook kan het zijn dat organisaties binnen deze sector een minder aantrekkelijk doelwit zijn omdat er relatief minder geld te halen is voor criminelen.

Tot slot is de respondenten gevraagd of ze deskundig zijn op gebied van de verschillende vormen van cybercriminaliteit. Uit de analyse blijkt dat 52% van de respondenten deskundige is op gebied van hacking, 50% van malware, 34% DDoS-aanvallen, 53% van phishing, 35% van social engineering, 55% van misbruik en 45% van ransomware. Om te kijken naar het belang van deze deskundigheid, is ook voor cybercriminaliteit een phi correlatie uitgevoerd.[2] Ook hier kan geconcludeerd worden dat onder respondenten met deskundigheid op het gebied van cybercriminaliteit vaker cybercriminaliteit wordt gerapporteerd dan onder respondenten zonder deskundigheid. ■

2 Hiervoor is een nieuwe variabele aangemaakt die aangeeft of de respondent wel of geen deskundige is. De phi correlatie coëfficiënt komt overeen met 0.181. Dit is een zwak positief verband.

3. Daders van financieel-economische criminaliteit

Daders van traditionele financieel-economische criminaliteit en cybercriminaliteit

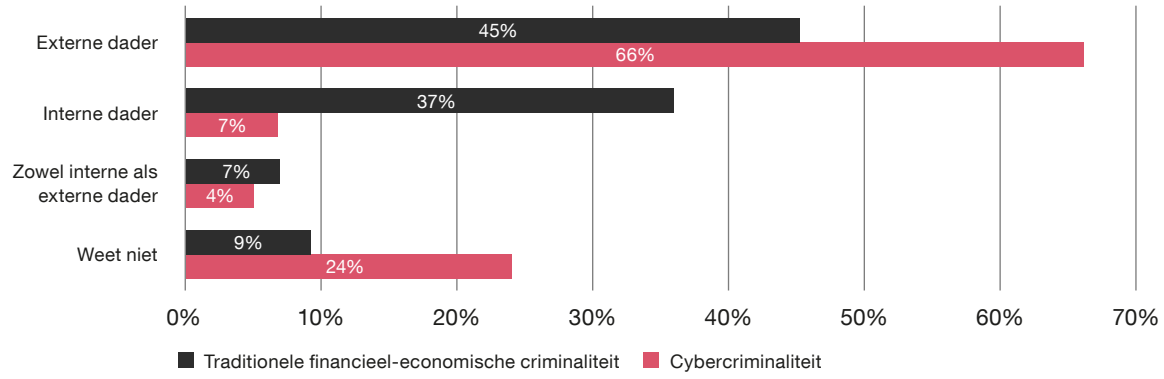
In de survey zijn enkele vragen gesteld met betrekking tot de dader van het meest ernstige delict dat de respondenten in de afgelopen twee jaar hebben ervaren. Dit is gedaan om een beeld te kunnen schetsen van het profiel van de dader. Zo is gevraagd of de dader ten tijde van het delict werkzaam was binnen de organisatie en of de dader van buiten de organisatie kwam. Daarbij is onderscheid gemaakt tussen daders van traditionele financieel-economische criminaliteit en cybercriminaliteit. De resultaten hiervan zullen in dit hoofdstuk uiteen worden gezet.

Uit *figuur 15* blijkt dat traditionele financieel-economische criminaliteit in 45% van de gevallen wordt gepleegd door een externe dader en in 37% door een interne dader. Bij cybercriminaliteit liggen deze verhoudingen een stuk verder uit elkaar. In 66% van de gevallen wordt het delict gepleegd door een externe dader en in 7% van de gevallen door een interne dader. Ook is te zien dat in een kwart van de gevallen van cybercriminaliteit onbekend is of er sprake is van een interne of externe dader. Dit komt overeen met de voorgaande edities van de Economic Crime Survey. Het hoge aantal externe daders kan verklaard worden door middel van het kenmerk 'time space compression' van cybercriminaliteit. Time-space compression houdt in dat tijd en ruimte wegvallen bij cybercriminaliteit (Van der Wagen et al., 2020). Waar het bij traditionele financieel-economische criminaliteit belangrijk kan zijn om fysiek en overdag aanwezig te zijn op een kantoor, kan cybercriminaliteit 's nachts gepleegd worden en zelfs vanuit een ander land. Dit maakt cybercriminaliteit vatbaarder voor externe daders. Daarentegen is de legitieme toegang van de dader tot het doelwit op plaats een kenmerk van gelegenheid tot witteboordencriminaliteit (Simpson & Benson, 2018) en daarmee een verklaring voor het hogere percentage interne daders bij traditionele financieel-economische criminaliteit.

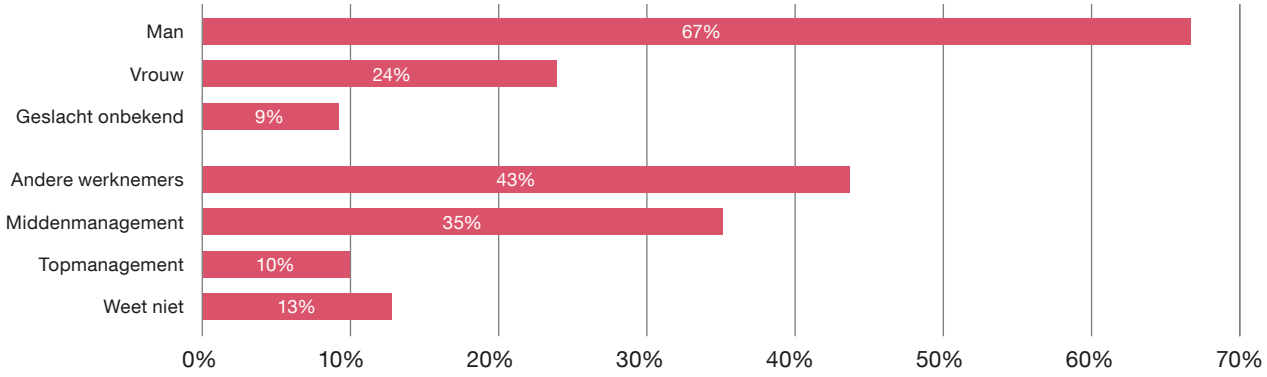
Verschillende experts nuanceren in de interviews het onderscheid tussen interne en externe daders. De arbeidsmarkt wordt steeds flexibeler en steeds meer organisaties maken gebruik van zzp'ers en andere ingehuurde krachten. Deze zzp'ers zouden zowel als interne als externe dader gekenmerkt kunnen worden. Een expert stelt daarbij: *''Er worden dus veel mensen ingehuurd, zowel in de uitvoering en op stafafdelingen. Het zijn dus daders die wel bij de organisatie horen, maar het is geen eigen personeel''*. Volgens deze expert kan deze flexibeler wordende arbeidsmarkt leiden tot een verhoogd risico op slachtofferschap van financieel-economische criminaliteit.

Dit zou enerzijds te maken kunnen hebben met een gebrek aan controle die een organisatie kan uitoefenen op zzp'ers. Anderzijds zou dit te maken kunnen hebben met het feit dat zzp'ers zich minder gebonden voelen aan de organisatie. Een andere expert van het OM vertelt hierover het volgende: *"Het is belangrijk als je een dienstverlening aangaat, je ook de eisen die je voor je eigen werknemer stelt op het gebied van toegangsbeheer en informatie ook stelt aan zzp'ers."*

Figuur 15 Verdeling interne en externe dader van het meest recente delict



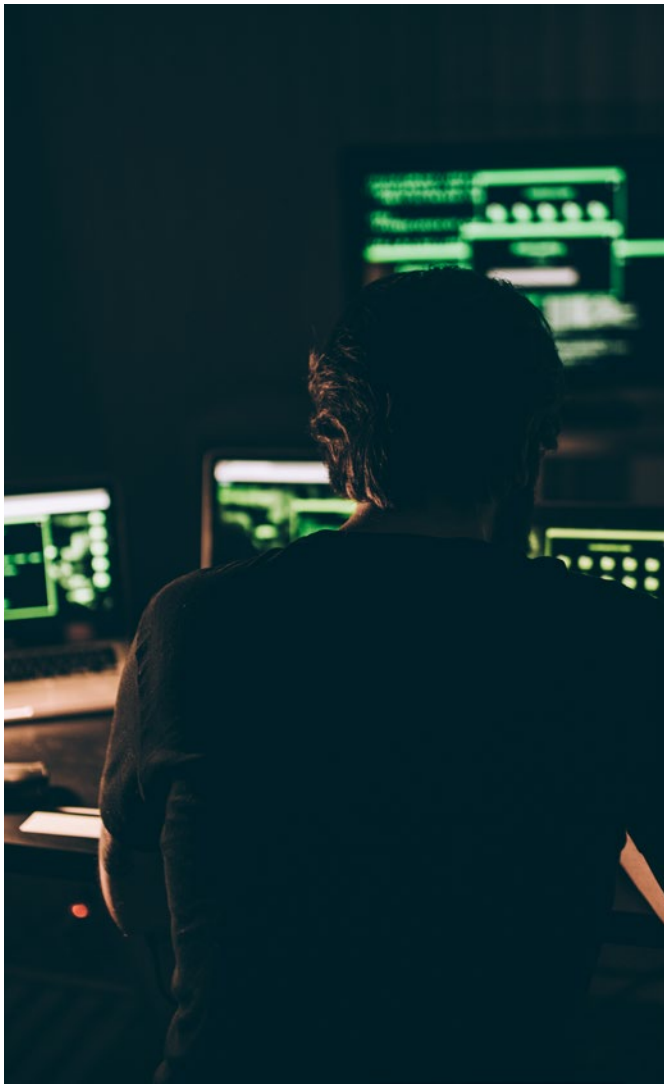
Figuur 16 Daderprofiel interne dader



Aan de hand van de vragen over daders kan een intern en een extern daderprofiel opgesteld worden. *Figuur 16* geeft het interne daderprofiel weer. Dit zijn de daders die werkzaam zijn in dezelfde organisatie als waar het strafbare feit is gepleegd. De gemiddelde leeftijd van een interne dader is 36 jaar. Verder blijkt dat 67% van daders mannelijk is en 24% vrouwelijk. Opvallend hierbij is dat het percentage vrouwelijke daders met 5% is gestegen ten opzichte van de vorige editie van de Economic Crime Survey. Uit de interviews met experts blijkt dat de stijging te maken zou kunnen hebben met het feit dat de arbeidsparticipatie van vrouwen is toegenomen. Toch blijft het traditionele verschil tussen mannen en vrouwen in daderschap nog steeds zichtbaar.

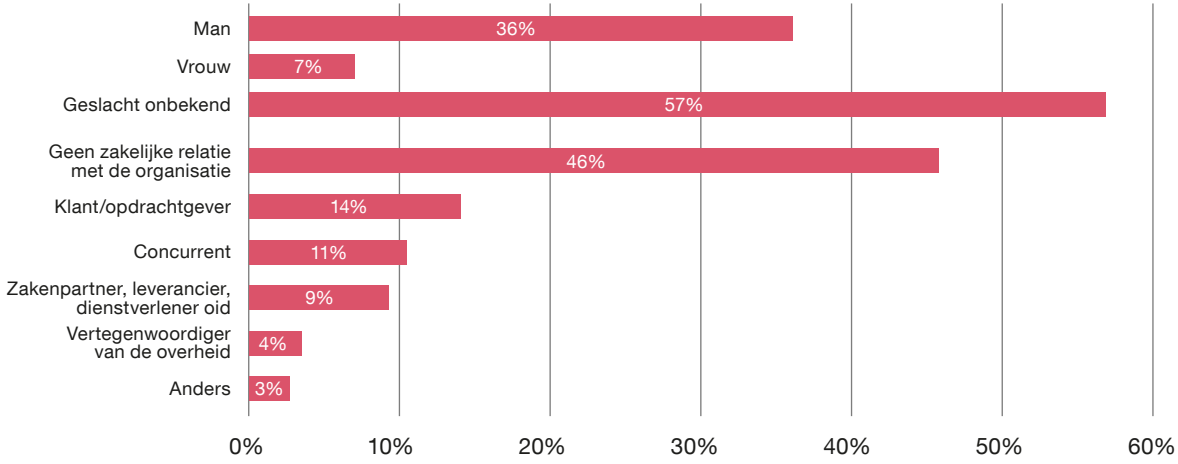
Een expert van de politie geeft tijdens het interview het volgende aan over het geslacht: *"Een groot deel van de daders is een man maar dit heeft ook te maken met bias. Tijdens de opsporing worden mannen ook eerder als dader beschouwd. Vrouwen worden juist minder snel als schuldig bevonden."*

Daarnaast is gevraagd in welke functie de interne dader werkzaam was. Hieruit blijkt dat slechts 10% van de daders afkomstig is uit het topmanagement. Het percentage daders uit het middenmanagement komt overeen met 35% en in 43% van de gevallen ging het om andere werknemers. Deze percentages komen overeen met de voorgaande editie.



In *figuur 17* is het externe daderprofiel te zien. Dit zijn de daders die niet in dienst zijn van de organisatie. De gemiddelde leeftijd van de externe dader is 35 jaar. Het geslacht van de externe dader is, conform voorgaande edities, in meer dan de helft van de gevallen onbekend. Tevens is de respondenten gevraagd naar de relatie met de dader. Hieruit blijkt dat in 46% van de gevallen de dader geen zakelijke relatie heeft met de organisatie die slachtoffer is geworden. De relatie waarin de dader een vertegenwoordiger is van een overheid die bijvoorbeeld om een steekpenning vraagt, wordt het minst vaak genoemd (4%). ■

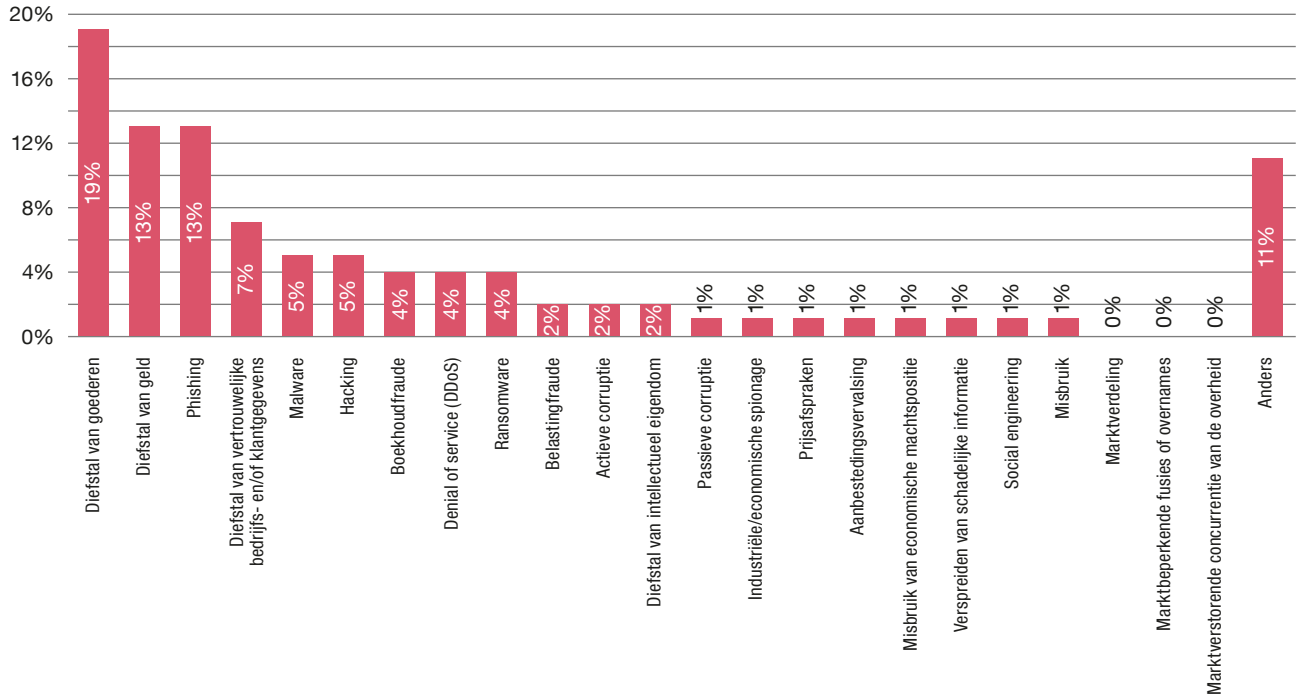
Figuur 17 Daderprofiel externe dader



4. Schade van financieel-economische criminaliteit

Schade van financieel-economische criminaliteit
In het voorgaande hoofdstuk is het daderprofiel van financieel-economische criminaliteit aan de orde gekomen. In dit hoofdstuk staat de schade centraal die traditionele financieel-economische criminaliteit en cybercriminaliteit veroorzaakt. Daarbij zijn aan de respondenten verschillende vragen omtrent schade gesteld. Ten eerste is gevraagd welke vorm van financieel-economische criminaliteit het meest ernstige is geweest in de afgelopen 2 jaar. Dit overzicht is terug te zien in *figuur 18*. Hieruit blijkt dat diefstal van goederen het vaakst wordt vermeld als meest ernstige geval van financieel-economische criminaliteit (19%). Deze vorm van criminaliteit wordt gevolgd door diefstal van geld en phishing, die beide door 13% van de respondenten worden gerapporteerd.

Figuur 18 Meest ernstige geval van financieel-economische criminaliteit in de afgelopen twee jaar

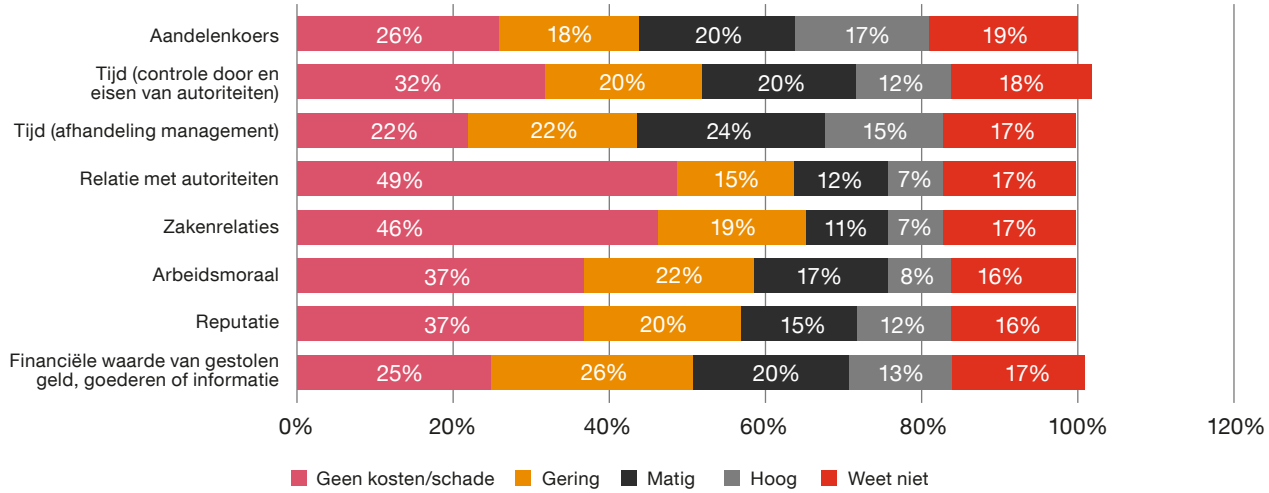


"De angst voor reputatieschade van veel bedrijven is schijnbaar groter dan de daadwerkelijke schade op dit gebied."

Ten tweede is de respondenten gevraagd wat zij denken wat het meest ernstige delict heeft gekost, inclusief eventuele onderzoeks- en proceskosten. Van de 875 respondenten hebben 288 respondenten hierop een antwoord gegeven. Het laagste bedrag dat werd vermeld was 5 euro en het hoogste bedrag was 100 miljoen euro. Omdat deze getallen zo ver uit elkaar liggen, is ervoor gekozen om ook de mediaan uit te rekenen. Bij gebruik van de mediaan wordt gecontroleerd voor uitbijters. De mediaan bedraagt 1500 euro schade als gevolg van slachtofferschap van het meest ernstige delict. De gemiddelde schade die respondenten vermelden bedraagt daarentegen 143.539 euro.

Ten derde is de respondenten gevraagd de mate van schade aan te geven op een schaal van 'geen schade' tot 'hoog'. Dit is voor traditionele financieel-economische criminaliteit en cybercriminaliteit afzonderlijk in kaart gebracht.

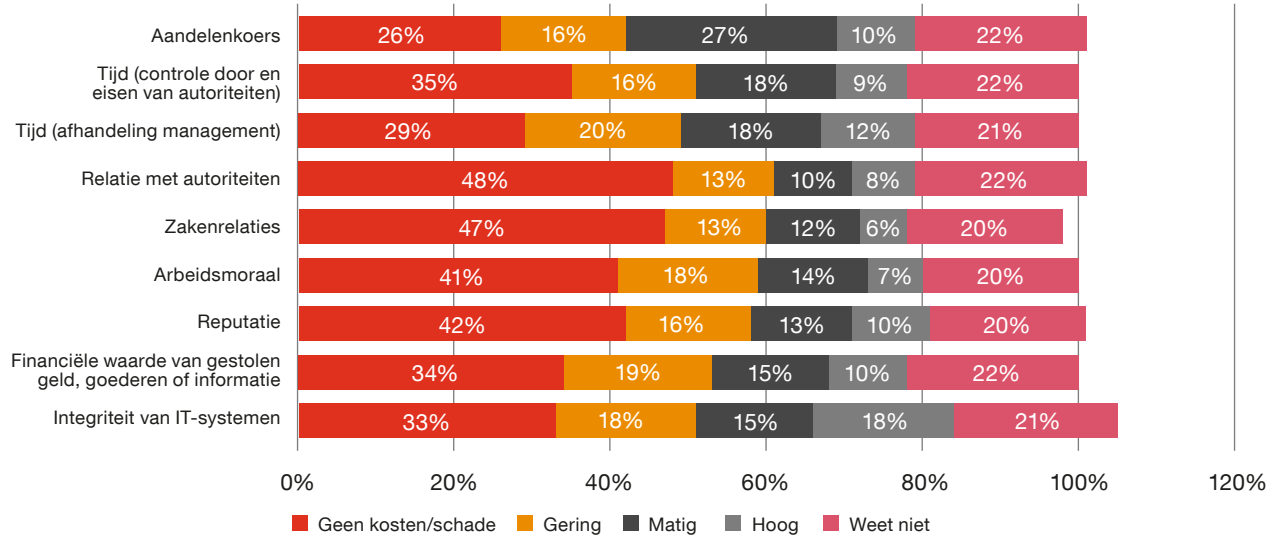
Figuur 19 Schade als gevolg van traditionele financieel-economische criminaliteit



In *figuur 19* is de schade als gevolg van traditionele financieel-economische criminaliteit met betrekking tot uiteenlopende onderwerpen zoals reputatie en arbeidsmoraal te zien. Hieruit blijkt dat de aandelenkoers op het gebied van schade van traditionele financieel-economische criminaliteit het vaakst als 'hoog' wordt gerapporteerd. Naast de financiële waarde van hetgeen onrechtmatig afgenomen is, rapporteren de respondenten ook relatief veel schade in de vorm van de tijd die gemoeid is met de interne en externe afhandeling van de gepleegde criminaliteit. De vorm van schade van traditionele financieel-economische criminaliteit die het vaakst met 'geen kosten' wordt vermeld is de relatie met de autoriteiten.

Een van de experts zegt hierover het volgende: *"De angst voor reputatieschade van veel bedrijven is schijnbaar groter dan de daadwerkelijke schade op dit gebied."*

Figuur 20 Schade als gevolg van cybercriminaliteit



In *figuur 20* is de schade van cybercriminaliteit weergegeven op uiteenlopende gebieden. Hieruit blijkt dat schade aan de integriteit van ICT-systemen het vaakst als 'hoog' (18%) wordt gerapporteerd. Verder komen de schadeposten overeen met die van traditionele financieel-economische criminaliteit. Dat de schade door de tijd die met de interne afhandeling door het management is gemoeid hoger is bij traditionele criminaliteit, kan mogelijk verklaard worden door het hogere percentage interne daders en de arbeidsrechtelijke procedures die hiermee gepaard gaan. Daarnaast zijn er bij interne daders meer onderzoeksmogelijkheden, waardoor het onderzoek vaak omvangrijker is.

Zo geeft een geïnterviewde expert aan: "*De afhandeling van het onderzoek is vaak een tijdrovende klus. Zeker als je te maken hebt met medewerkers die ontslagen worden en als gevolg daarvan een advocaat inhuren''*.

Tenslotte is de respondenten gevraagd naar wie het slachtoffer is geweest van het meest recente geval van financieel-economische criminaliteit en cybercriminaliteit in de afgelopen 2 jaar. Hieruit blijkt dat de organisatie voor zowel traditionele financieel-economische criminaliteit (67%) en cybercriminaliteit (57%) het meest wordt gerapporteerd.

Een expert uit de interviews legt uit dat vooral in de financiële sector de organisatie vaak indirect slachtoffer is. Dat komt volgens de experts doordat de schade die individuele klanten oplopen als gevolg van financieel-economische criminaliteit in bepaalde gevallen vergoed wordt door de bank. Hierdoor neemt de bank uiteindelijk de financiële schade voor zijn rekening.

Ten aanzien van cybercriminaliteit vertellen experts dat hoewel 21% van de respondenten aangeeft dat een individuele medewerker het slachtoffer van cybercriminaliteit is, het in die gevallen ook zo kan zijn dat de organisatie het eigenlijke doelwit van cybercriminelen was en dat zij via de smartphone of email van die medewerker toegang probeerden te krijgen tot de organisatie. ■

5. Detectie van financieel-economische criminaliteit

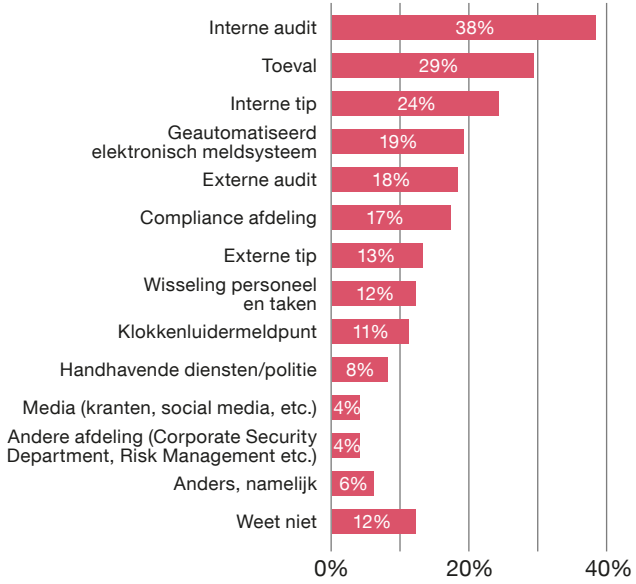
In de vorige hoofdstukken is opgemerkt dat traditionele financieel-economische criminaliteit en cybercriminaliteit veelal gedaald zijn ten opzichte van de voorgaande editie van de Economic Crime Survey. Om die reden is het interessant om te kijken naar de detectie van financieel-economische criminaliteit. Zijn hier veranderingen waar te nemen die de bevindingen uit de voorgaande hoofdstukken (deels) kunnen verklaren?

Payne (2018) schrijft dat bijvoorbeeld cybercriminaliteit kampt met een hoog dark number. Dit komt mede doordat men niet altijd weet dat men slachtoffer is geworden (Van der Wagen et al., 2020). Iets soortgelijks geldt voor traditionele financieel-economische criminaliteit dat vaak verhuld wordt als reguliere zakelijke transacties (Simpson & Benson, 2018). Kwaadaardige software kan zich nestelen in een computer zonder dat het 'slachtoffer' het doorheeft. Om die reden is het belangrijk om als organisatie voldoende detectiemethoden te hebben.

Figuur 21 laat zien op welke verschillende manieren traditionele financieel-economische criminaliteit binnen een organisatie aan het licht kunnen komen. Evenals vorig jaar komen de meeste delicten boven water door interne audit, namelijk 38%. Voor detectie van criminaliteit wordt door veel organisaties het 'three lines of defence'-model gebruikt (IIA, 2013). Binnen dit model wordt de derde verdedigingslinie gevormd door interne audit. De eerste lijn van het model bestaat uit het management en de maatregelen die getroffen worden in het operationele proces. De tweede lijn bestaat uit steunmaatregelen die de business beschermen en controleren zoals compliance. Na de interne audit rapporteren respondenten detectiemethoden die weinig met eigen beleid en organisatie te maken lijken te hebben, waaronder toeval, interne en externe tips en externe audit.

De eerste twee lijnen lijken daarmee minder goed te werken. Detectie door compliance is in deze editie gestegen van 14% in 2019 naar 17% in 2021. De detectie maatregel die het meest gedaald is ten opzichte van 2019 is de interne tip. Deze bron is afgenomen van 31% in 2019 naar 24% in 2021. Vermoedelijk kan de coronacrisis een verklaring bieden voor deze uitkomst. Het thuiswerken kan ertoe

Figuur 21 Hoe komen vormen van traditionele financieel-economische criminaliteit binnen uw organisatie doorgaans aan het licht?



leiden dat minder contact is met collega's wat een negatieve invloed kan uitoefenen op de 'interne tip'. Daarnaast blijkt uit het kwalitatieve onderzoek dat bij 'interne tip' de bewustwording inzake financieel-economische criminaliteit binnen een organisatie een belangrijke rol speelt. Een van de geïnterviewde experts vertelt: *"Interne tips komen voornamelijk naar voren als er een hoog bewustzijn is binnen de organisatie van frauderisico's"*. Een andere expert wijst erop dat interne tips gezien kunnen worden als de

werking van de eerste lijn: de verantwoordelijkheid van het management bewustzijn en een cultuur te creëren waarin medewerkers misstanden melden.

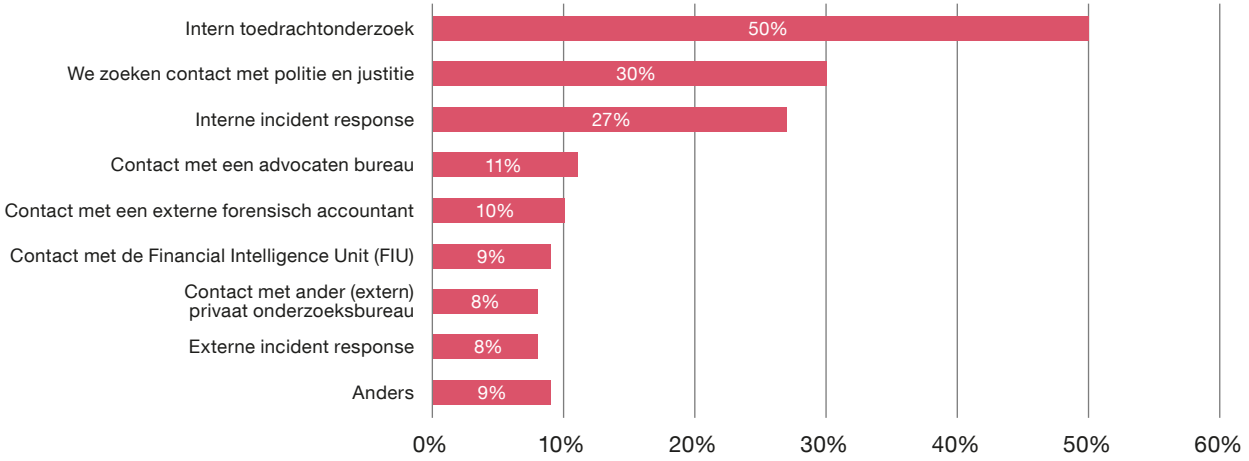
Ook zijn dit jaar correlaties berekend om de samenhang vast te stellen tussen de verschillende detectiemethoden en de prevalentie van traditionele financieel-economische criminaliteit en cybercriminaliteit.

Voor traditionele financieel-economische criminaliteit zijn zwakke positieve correlaties gevonden voor klokkenluidermeldpunt (0.119), externe tip (0.088), interne tip (0.156), wisseling van personeel en taken (0.154) en handhavende diensten/politie (0.115).

Met betrekking tot de prevalentie van cybercriminaliteit zijn zwakke positieve correlaties gevonden voor interne audit (0.129), externe audit (0.133), compliance (0.144), geautomatiseerd elektronisch meldsysteem (0.165), klokkenluidermeldpunt (0.117) en externe tip (0.145).

Hieruit kan geconcludeerd worden dat wanneer een organisatie in bezit is van één van de hierboven genoemde detectiemethoden, zij vaker financieel-economische criminaliteit rapporteren. Dit kan verklaard worden door middel van de controle-paradox. Deze controle-paradox houdt in dat wanneer beter gecontroleerd wordt op financieel-economische criminaliteit, ook meer criminaliteit aan het licht komt (Hardy & Levine, 2018). Het gaat echter in alle gevallen wel om zwakke verbanden. Daarom dient wel de kanttekening gemaakt te worden dat het verband ook

Figuur 22 Welke actie's onderneemt u als traditionele financieel-economische criminaliteit en cybercriminaliteit aan het licht komt?

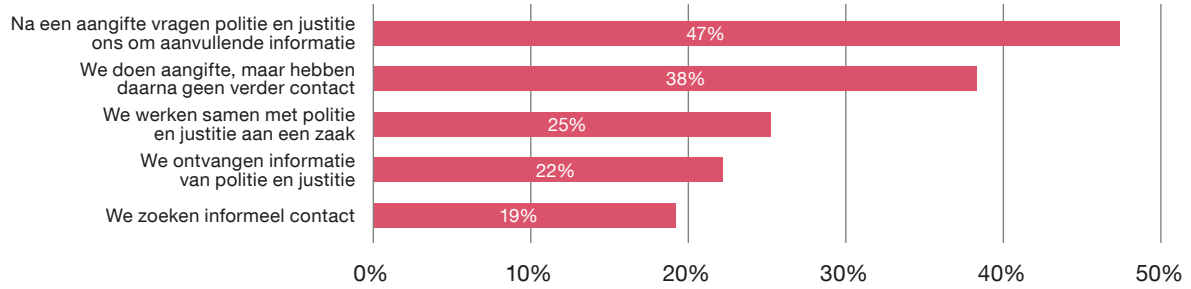


beïnvloed kan zijn door factoren die niet meegenomen zijn in de Economic Crime Survey.

In 2019 is voor het eerst gevraagd welke acties ondernomen zijn op het moment dat financieel-economische criminaliteit ontdekt wordt. De resultaten zijn weergegeven in *figuur 22*. Intern toedrachtonderzoek is voor 50% van de respondenten een vervolgstap na de constatering van criminaliteit. Een ander veelvoorkomende actie is interne incident response, dat bij 27% van de respondenten gebruikt wordt. Incident response is een methode die gebruikt wordt om een cyberaanval te controleren en te bestrijden. In het geval van intern incident response wordt dit uitgevoerd door een interne deskundige en bij externe incident response door een externe deskundige. Niet alleen intern uitgevoerde acties worden veel gebruikt. 30% van de respondenten zoekt na de ontdekking van de vorm van criminaliteit contact met politie en justitie. De uitkomsten voor de overige acties liggen aanzienlijk lager en redelijk in lijn met de uitkomsten van twee jaar geleden.

Zoals eerder in onderzoek is vastgesteld (Meerts, 2018), doen organisaties lang niet altijd aangifte van ondervonden financieel-economische criminaliteit: 30% zoekt contact met strafrechtelijke autoriteiten. Een van de experts van de politie merkt over de aangiftebereidheid het volgende op: *"We horen ook van partijen dat bedrijven bang zijn om*

Figuur 23 Op welke wijze heeft u contact met politie en justitie bij een geval van financieel-economische criminaliteit?

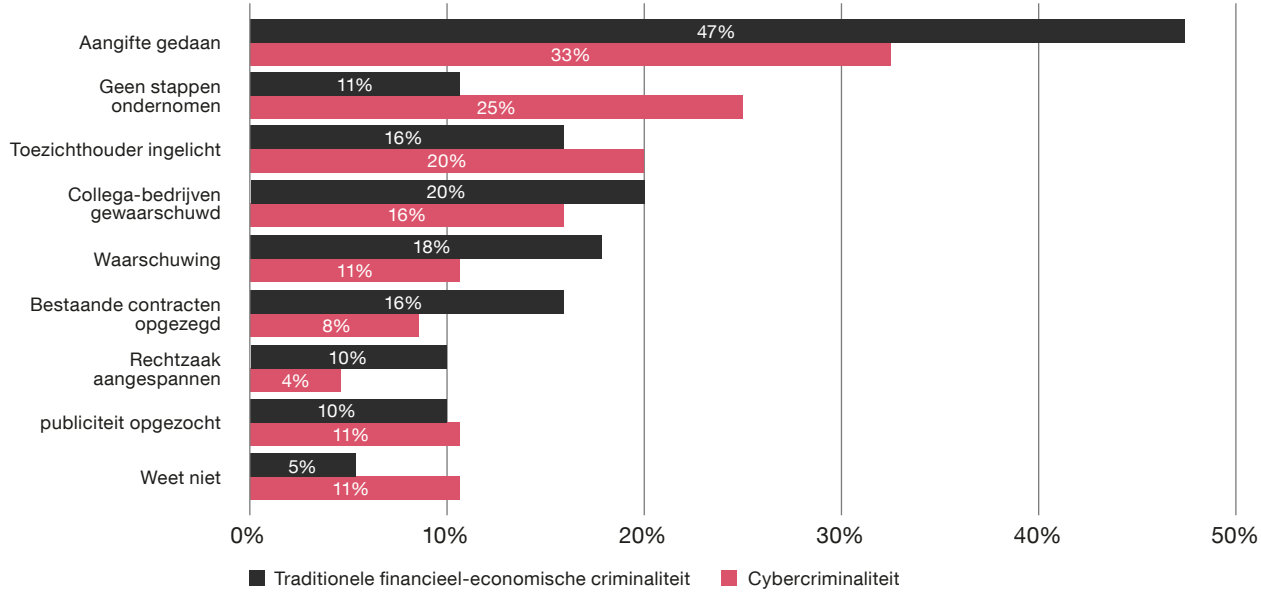


van 2019. 'Na aangifte vragen politie en justitie ons om aanvullende informatie' is dit jaar de meest voorkomende manier waarop met de politie en justitie contact was (47%). Twee jaar geleden kwam dit bij 40% van de respondenten voor. Het doen van aangifte, maar vervolgens 'geen verder contact hebben' wordt door 38% van de respondenten gerapporteerd. Daarmee is dit gedaald met 4%. In de editie van 2019 lagen deze twee vormen van contact dichter bij elkaar en kwam 'geen contact' vaker voor dan 'gevraagd worden door politie en justitie om aanvullende informatie te leveren'. De overige vormen van contact met politie en justitie liggen in lijn met de bevindingen uit de voorgaande editie.

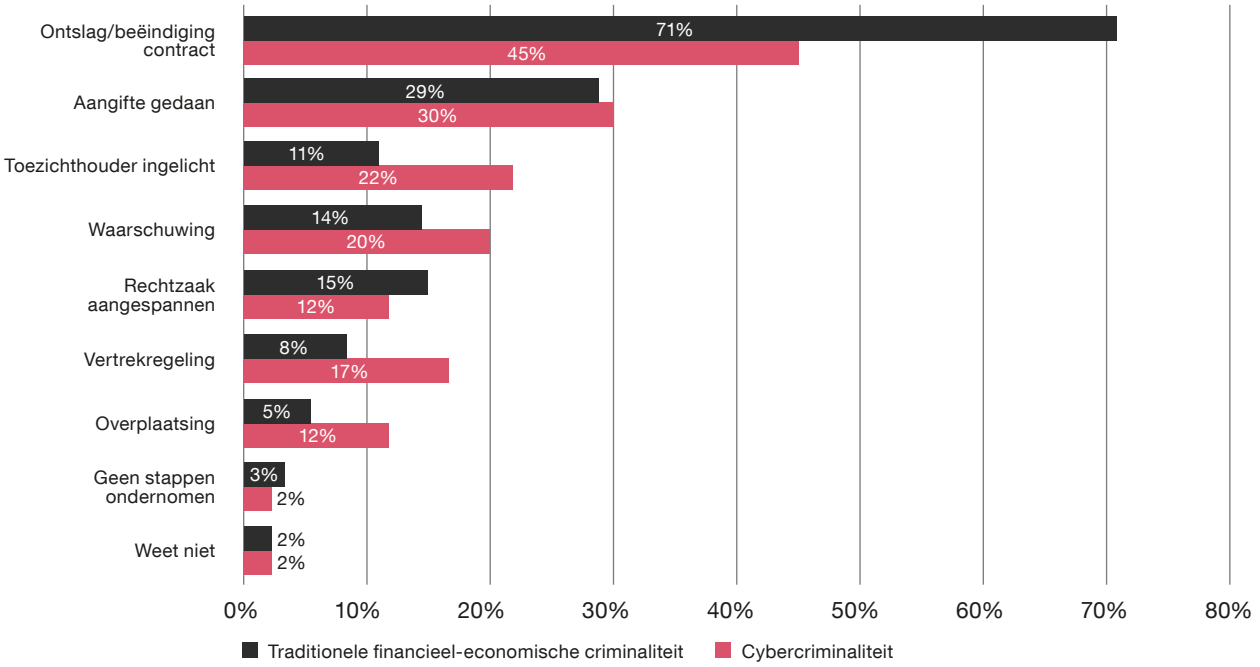
imagoschade op te lopen, zeker als ze beursgenoteerd zijn. Wij kunnen in overleg met het OM aangeven dat de bedrijven anoniem wensen te blijven maar ze zijn vaak toch bang dat het lekt en dat is volgens mij een van de redenen waarom er zo weinig aangiftes worden gedaan vanuit bedrijven.".
Uit de afgenomen interviews blijkt daarnaast dat het per situatie sterk kan verschillen welke vervolgstappen ondernomen worden. Meerdere experts vertellen dat voordat (eventuele) aangifte gedaan wordt, eerst intern onderzoek gedaan wordt (zie ook Meerts, 2018). Daarnaast stelt een van de experts dat: *"het afgeven van een signaal ter afschrikking soms belangrijker is dan de kosten. De gemaakte kosten voor het interne onderzoek waren hoger dan de geleden schade". "Maar het afgeven van een signaal en de preventie is nog belangrijker"*, vertelt de expert.

Onder de respondenten, die na detectie van financieel-economische criminaliteit contact zochten met politie en justitie, is een vervolgvraag gesteld. De uitkomsten uit *figuur 23* liggen niet geheel in lijn met de resultaten

Figuur 24 Gevolgen externe dader meest recente delict



Figuur 25 Gevolgen interne dader meest recente delict



Detectie van financieel-economische criminaliteit ziet niet alleen toe op handelingen met betrekking tot opheldering van het delict. Het betreft ook de gevolgen die de detectie heeft voor de dader van financieel-economische criminaliteit. In de Economic Crime Survey zijn daders van financieel-economische criminaliteit ingedeeld in externe en interne daders. In *figuur 24* zijn de desbetreffende gevolgen voor de externe dader weergegeven bij het meest recente delict. Net als in de voorgaande editie werd het vaakst aangifte gedaan. Bij cybercriminaliteit gebeurde dit bij 33% van de gevallen en bij traditionele financieel-economische criminaliteit bij 47% van de gevallen. Daarnaast wordt bij cybercriminaliteit aanzienlijk vaker geen stappen ondernomen. Van de Weijer, Leukfeldt en Van der Zee (2020) stellen dat de aangiftebereidheid bij cybercriminaliteit lager is, omdat de pakkans lager is en men het vaker zelf kan oplossen. Om die reden zullen slachtoffers van cybercriminaliteit minder snel overgaan tot het doen van aangifte.

In *figuur 25* zijn de gevolgen voor interne daders van het meest recente delict weergegeven. Ontslag/beëindiging van het contract komt het meeste voor. Bij traditionele financieel-economische criminaliteit gebeurde dit zelfs bij 71% van de respondenten, een lichte stijging ten opzichte van 2019. Daarnaast werd in 2021 vaker een toezichthouder ingelicht bij cybercriminaliteit dan in 2019. In 22% van de gevallen werd bij cybercriminaliteit een toezichthouder ingelicht in 2021, terwijl in 2019 dit aantal nog op 10% lag.

Data-analyse

Digitalisering zorgt voor ingrijpende ontwikkelingen in de samenleving, ook binnen het forensisch werkveld. Door de jaren heen kunnen steeds grotere hoeveelheden data geanalyseerd worden in de opsporing van financieel-economische delicten.

Gelet op het toenemende belang van het gebruik van data-analyse is aan de respondenten gevraagd of binnen hun organisatie gebruik wordt gemaakt van data-analyse bij het detecteren van financieel-economische criminaliteit. De uitkomsten zijn weergegeven in *figuur 26*. Hieruit blijkt dat 28% van de respondenten gebruik maakt van data-analyse bij het detecteren van financieel-economische criminaliteit. Dit betreft een lichte stijging van 3% ten opzichte van de editie uit 2019. Het overgrote deel (39%) daarentegen geeft aan geen gebruik te maken van data-analyse. Dit is echter een lager percentage dan twee jaar geleden. Dit betekent dat het gebruik van data-analyse voor detectie van financieel-economische criminaliteit in opkomst is.

“Data is het nieuwe olie.”

9% geeft aan in de toekomst gebruik te willen maken van data-analyse. Daarnaast zijn phi-correlaties uitgedraaid tussen het al dan niet gebruiken van data-analyse en traditionele financieel-economische criminaliteit en cybercriminaliteit.

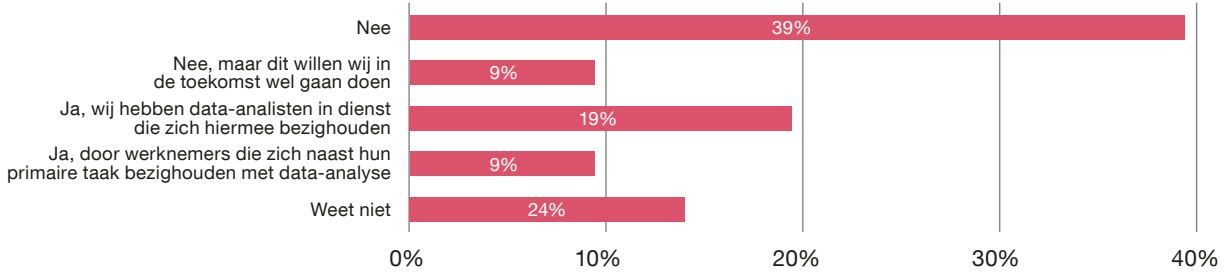
Twee zwakke positieve verbanden zijn gevonden tussen het gebruik van data-analyse en de prevalentie van traditionele financieel-economische criminaliteit (0.194) en cybercriminaliteit (0.197). Geconcludeerd kan worden dat organisaties die gebruik maken van data-analyse vaker financieel-economische criminaliteit ontdekken en rapporteren.

Uit de interviews is een wisselend beeld ontstaan over het gebruik van data-analyse. Meerdere respondenten geven aan op dit moment binnen hun organisatie gebruik te maken van data-analyse, maar dit niet altijd in te zetten in de detectie van financieel-economische criminaliteit. Daar staat tegenover dat experts uit andere sectoren al volop gebruik maken van data-analyse in het detecteren van criminaliteit. *“De laatste werknemer die ik heb aangenomen in mijn team is een data analist”.* Vervolgens vertelt de expert: *“Data-analyse gaat steeds beter en de ambitie is om besluiten te nemen gebaseerd op 80% van geautomatiseerde data-analyse en 20% uit professional judgement.”*

Aangezien data-analyse een nogal ruim begrip is, is het in de survey vervolgens nader uiteengezet in verschillende manieren van data-analyse. Daarnaast is deze uiteenzetting verder uitgebreid ten opzichte van de voorgaande editie van de Economic Crime Survey. Naast vormen van data mining, data integratie en data visualisatie is ook gevraagd naar het gebruik van threat intelligence, webmonitoring en threat assessment. Threat intelligence is gericht op het tijdig informatie verkrijgen van dreigingsactoren en mogelijke cyberaanvallen (Dehghantanha, Conti en Dargahi, 2018). Hierbij kan onderscheid worden gemaakt tussen technische threat intelligence en strategische threat intelligence. Technische threat intelligence omvat de ‘technische’ informatie zoals de middelen die gebruikt worden voor het plegen van een cyberaanval zoals IP-adressen. Strategische threat intelligence omvat de informatie die geïnformeerde, *risk based*, beslissingen mogelijk maakt. Webmonitoring geeft extra inzicht in het digitale dreigingsgevaar voor organisaties. Dit kan bijvoorbeeld gaan om informatie op het internet over gelekte wachtwoorden van medewerkers. Tot slot is threat assessment een beoordeling van dreigingen voor een organisatie en dreigingsomgeving over een breed traject. Deze beoordeling biedt vervolgens de mogelijkheid om nieuwe bedreigingen voor te zijn.

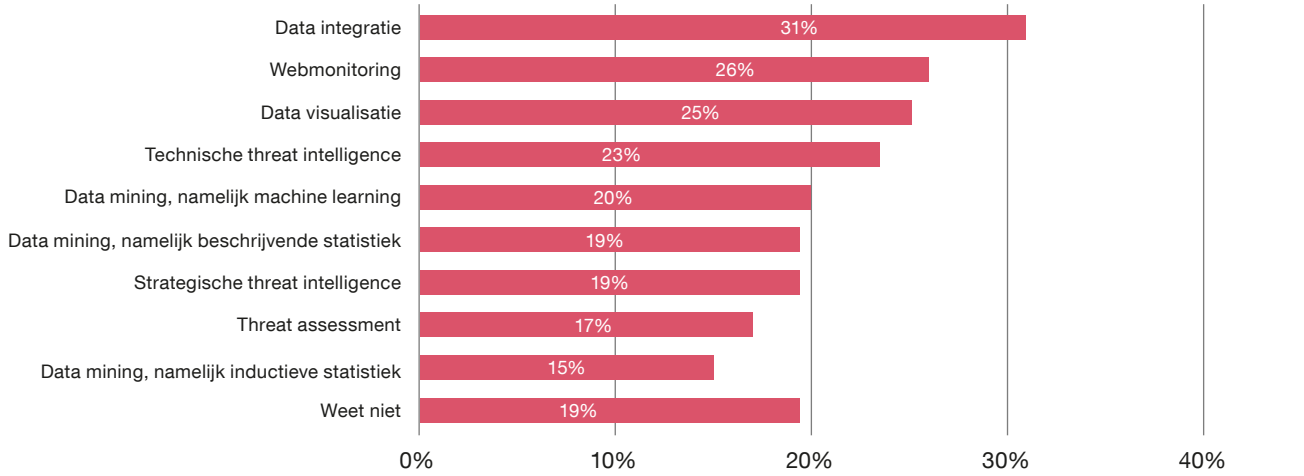
Figuur 27 laat zien dat het meest gebruik wordt gemaakt van data-integratie[3], namelijk door 31% van de respondenten. Dit wordt gevolgd door webmonitoring met 26%. Dit gaat gepaard met een daling van het gebruik van beschrijvende statistiek. Dit jaar werd dit door 19% van de respondenten ingezet waar dit vorig jaar nog door 34% was. Ook inductieve statistiek[4] is in deze editie gedaald van 29% naar 15%. Daarmee worden deze vormen niet enkel in omvang voorbijgestreefd door webmonitoring, maar ook door threat intelligence. Technische threat intelligence wordt door 23% van de respondenten gebruikt en strategische door 19%. Het hierboven beschreven threat assessment komt bij 19% van de ondervraagden voor. De overige uitkomsten, zoals weergegeven in figuur 27 komen overeen met het beeld dat is geschetst in de vorige editie. Hierbij dient echter een kanttekening gemaakt te worden. Door het toevoegen van een extra antwoordcategorie voor data-analyse is het vergelijken met 2019 gecompliceerder.

Figuur 26 Maakt u momenteel gebruik van data-analyse?



3 Het koppelen van databestanden voor nieuwe inzichten.
4 Specifieke waarnemingen generaliseren naar een algemene regel (bottom-up).

Figuur 27 Op welke manier wordt gebruik gemaakt van data-analyse bij het detecteren van traditionele financieel-economische criminaliteit en cybercriminaliteit?



Daarnaast is ook gekeken of het gebruik van threat-intelligence samenhangt met de prevalentie van traditionele financieel-economische criminaliteit en cybercriminaliteit. Uit de phi-correlatie is gebleken dat voor zowel traditionele financieel-economische criminaliteit (0.145) als cybercriminaliteit (0.241) een zwak positief verband bestaat. Daarom kan geconcludeerd worden dat organisaties die gebruik maken van threat-intelligence vaker traditionele financieel-economische criminaliteit en cybercriminaliteit rapporteren. Net als bij de uitkomsten van de correlaties voor detectiemethoden, kan ook dit verklaard worden door middel van de controle-paradox. Opvallend is dat threat intelligence, dat informatie verschaft over mogelijke cyberdreigingen, ook samenhangt met de prevalentie van traditionele financieel-economische criminaliteit.

Tijdens de interviews met de experts komt ook de *bias* van mogelijke algoritmen naar voren en hierover worden ook enige zorgen uitgesproken. ‘Machine learning’ is een toepassing van ‘Artificial Intelligence’ (AI) waardoor computers data kunnen bereiken, verwerken en zelf hiervan kunnen leren, zonder dat voor het verdere leerproces aanvullend programmeren nodig is. Aan de basis van ‘machine learning’ ligt een algoritme. Een algoritme is een reeks instructies die steeds weer wordt toegepast op een min of meer vastgestelde set van data (Bleker-van Eyk,

“De laatste werknemer die ik heb aangenomen in mijn team is een data analist”

2020). Een mogelijk gevaar binnen een algoritme is een bias. Dit houdt in dat er in de reeks van instructies (onbedoelde) onzorgvuldigheden zijn geslopen. Dit heeft het effect dat bij iedere berekening van het algoritme een fout optreedt.

Uit een van de interviews met de experts komt het volgende naar voren: *“Het is ook van belang dat er toezicht is op data-analyse, anders kunnen vooroordelen ontstaan in bepaalde algoritmen zoals bij de toeslagen affaire.”* Een andere expert geeft aan dat ze binnen hun organisatie bezig zijn met het toezicht op data-analyse. *“Ook worden discussies gevoerd hoever je mag gaan met data-analyse. Hierbij moet men scherp zijn op welke methodiek toegepast wordt, anders kan het algoritme (mogelijk) op basis van ras uiteindelijk op een bepaalde uitkomst komen en dat is niet de bedoeling.”*

6. Preventie van financieel-economische criminaliteit

In dit hoofdstuk staat de preventie van financieel-economische criminaliteit centraal. Hierbij zal worden gekeken naar preventieve maatregelen die organisaties kunnen implementeren om financieel-economische criminaliteit te voorkomen. Daarnaast zal dieper ingegaan worden op een compliance programma en de relatie met financieel-economische criminaliteit.

In *figuur 28* is de mate waarin diverse preventieve maatregelen bij respondenten voorkomen of voor komend jaar op de planning staan, weergegeven.

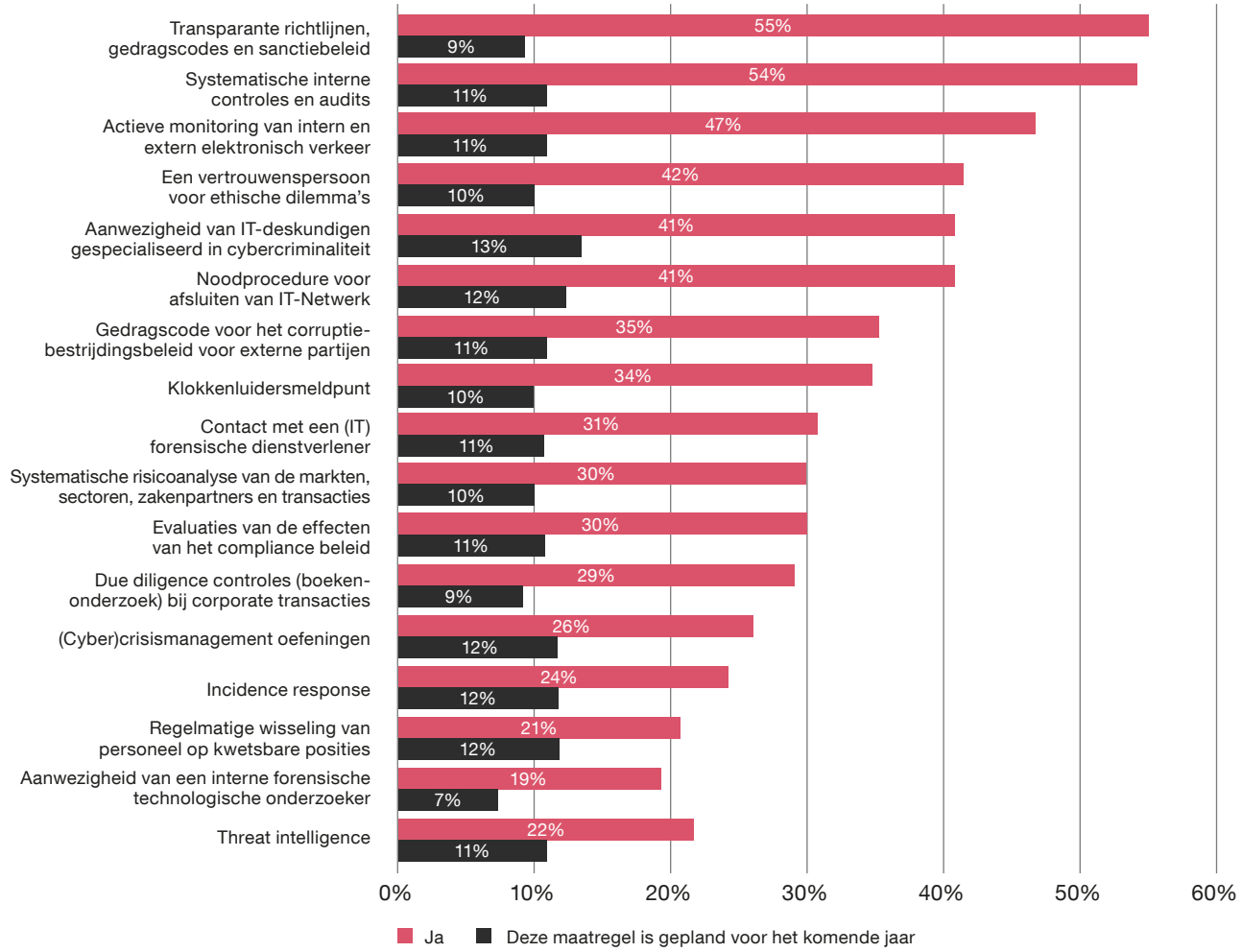
De meest voorkomende preventieve maatregelen zijn transparante richtlijnen, gedragscodes en sanctiebeleid (55%), systematische interne controles en audits (54%) en actieve monitoring van intern en extern elektronisch verkeer (47%). Alle drie de bovenstaande maatregelen hebben een daling meegemaakt ten opzichte van de uitslag uit 2019. Het beeld van dalende cijfers gaat echter niet voor alle categorieën op omdat sommige maatregelen nu vaker voorkomen dan in 2019. Deze maatregelen betreffen onder meer het hebben van een klokkenluidersmeldpunt die van 28% steeg naar 34% en contact met een (IT) forensisch dienstverlener die van 25% in 2019 naar 31% in 2021 steeg. Ook zijn nieuwe maatregelen aan de typologie toegevoegd, namelijk threat intelligence en incident response. 22% van de respondenten geeft aan threat intelligence te gebruiken om financieel-economische criminaliteit tegen te gaan en 24% doet dat door middel van incident response.

Een van de experts van de politie merkt op dat het aantal respondenten dat 'ja' invult bij de preventieve maatregelen uit figuur 28 laag is: *"Ik vind het schrikbarend laag, het aantal mensen dat hier 'ja' invult. Ook horen wij vaak dat mensen dit soort maatregelen te veel vinden kosten en er te lang mee wachten."* Hieraan wordt toegevoegd dat er wel een verandering waarneembaar is waarbij bedrijven inmiddels wel weten dat ze de preventieve maatregelen op orde moeten hebben en dat dit vroeger niet altijd vanzelfsprekend was.

Er is een significant gevonden voor de volgende preventiemaatregelen:

- Contact met een (IT) forensische dienstverlener/ incident response leverancier
- (cyber)crisis management oefeningen
- Threat intelligence; Incidence response
- Een noodprocedure voor het afsluiten van het IT-netwerk
- Aanwezigheid van IT-deskundigen gespecialiseerd in het voorkomen en bestrijden van cybercriminaliteit
- Evaluaties van de effecten van het compliance beleid
- Gedragscode voor het corruptiebestrijdingsbeleid voor externe partijen
- Klokkenluidersmeldpunt
- Een vertrouwenspersoon voor ethische dilemma's; Due-Diligence controles (boekenonderzoek) bij corporate transacties; Systematische risicoanalyse van de markten, sectoren, zakenpartners en transacties
- Actieve monitoring van intern en extern elektronisch verkeer
- Systematische interne controles en audits
- Transparante richtlijnen, gedragscodes en sanctiebeleid
- Regelmatige wisseling van personeel op kwetsbare posities
- Aanwezigheid van een interne forensisch technologisch onderzoeker.

Figuur 28 Heeft uw organisatie de volgende maatregelen getroffen om financieel-economische criminaliteit tegen te gaan?



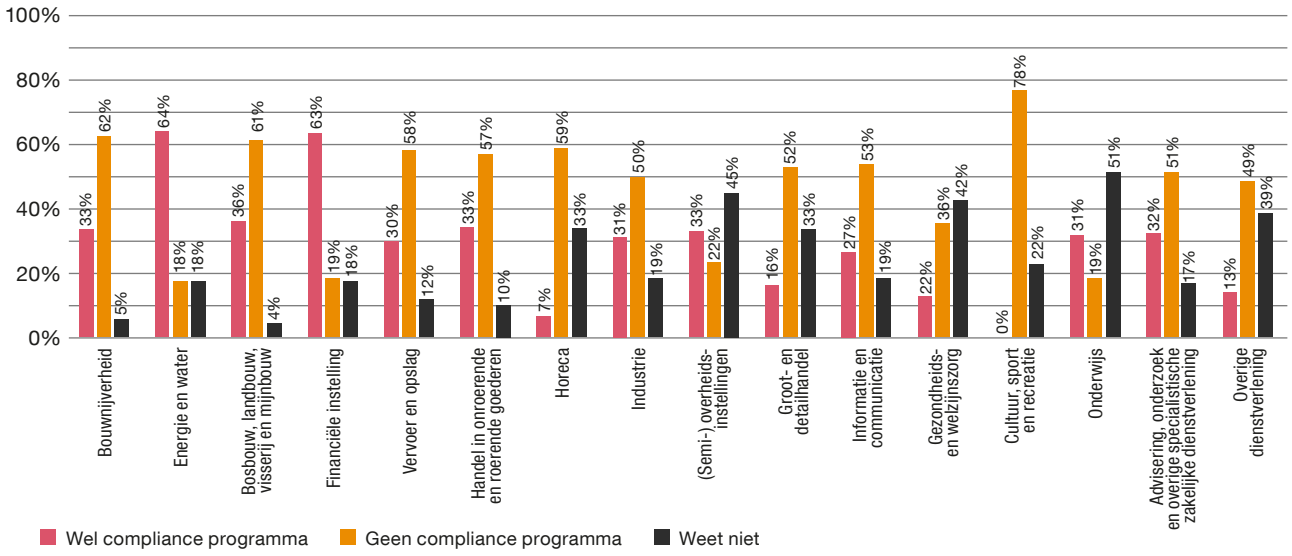
Daarnaast zijn dit jaar ook correlaties uitgedraaid voor de preventiemaatregelen en de prevalentie traditionele financieel-economische criminaliteit en cybercriminaliteit. Dit heeft een aantal positief zwakke significante verbanden opgeleverd voor zowel traditionele financieel-economische criminaliteit als cybercriminaliteit. De correlatie-coëfficiënten liggen alleen tussen de 0.191 en de 0.295. Hieruit kan geconcludeerd worden dat organisaties met de desbetreffende preventiemaatregelen, vaker financieel-economische criminaliteit rapporteren.

Hierbij is het opvallend dat dezelfde preventiemaatregelen significant zijn voor zowel traditionele financieel-economische criminaliteit als cybercriminaliteit. Dit houdt in dat maatregelen als 'threat intelligence', die gericht zijn op cybercriminaliteit, ook samenhangen met traditionele financieel-economische criminaliteit. Daar staat tegenover dat maatregelen als 'gedragscode voor het corruptiebestrijdingsbeleid voor externe partijen', die dienen als preventiemaatregel voor traditionele financieel-economische criminaliteit, ook significant zijn voor cybercriminaliteit. Dit kan een voorbeeld zijn van het spillover effect. Hierbij treden de preventiemaatregelen buiten hun verwachte kaders en hebben deze ook effect voor de 'andere' vorm van financieel-economische criminaliteit. Dit kan te maken hebben met een bepaalde bewustwording of cultuur binnen de organisatie waarbij er veel aandacht is preventiemaatregelen en de effectiviteit van de maatregelen groter is. Daarnaast kan het ook gaan om een 'spurieus verband'. Dit houdt in dat aan dit verband een achterliggende oorzaak zit, die in het huidige onderzoek niet is gemeten.

Een andere maatregel is het hebben van een klokkenluidersmeldpunt. Een expert geeft aan dat de stijging van het gebruik van een klokkenluidersmeldpunt het gevolg kan zijn van de invoering van de Wet bescherming klokkenluiders die in december 2021 van kracht wordt en bedrijven met meer dan 50 werknemers verplicht zo'n systeem te hebben: *"Het zou daarom zo kunnen zijn dat organisaties hier nu alvast op in spelen"* (Rijksoverheid, 2021).

Een andere opvallende trend is dat de vier meest voorkomende maatregelen uit 2019 allen gedaald zijn in deze editie van de Economic Crime Survey. Echter is er bij de overige maatregelen met lagere prevalenties een lichte stijging waar te nemen is. Daarnaast hebben relatief minder respondenten voornemens om komend jaar maatregelen tegen financieel economische criminaliteit in te voeren. Door de coronacrisis hebben veel organisaties andere financiële prioriteiten. Dit kan er mogelijk toe leiden dat het budget elders noodzakelijk wordt geacht en dat het invoeren van extra preventiemaatregelen op een lager pitje is komen te staan. De juiste balans vinden tussen business doelen, compliance en risico's is lastig voor organisaties (Sadiq & Governatori, 2015).

Figuur 29 Compliance programma per sector

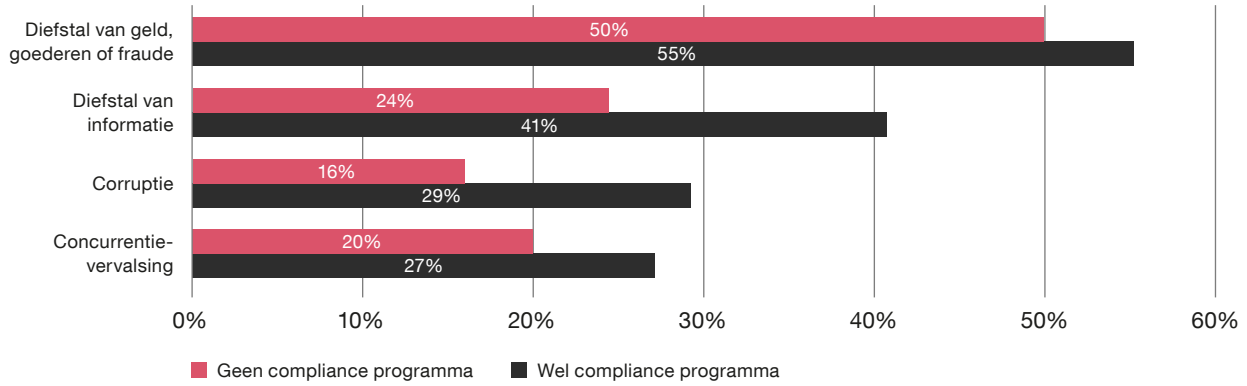


Compliance programma

De afgelopen jaren wordt onder andere door nieuwe wetgeving het belang van een compliance programma steeds meer benadrukt. Het aantal organisaties met een compliance programma is licht gestegen ten opzichte van de voorgaande editie. Deze stijging van 3% ligt dan ook in de lijn der verwachting. Dit jaar geeft 29% van de respondenten aan dat hun organisatie beschikt over een compliance programma.
Daarnaast verschilt het al dan niet hebben van een compliance programma per sector. Verschillen kunnen samenhangen met sectorspecifieke wetgeving of certificeringsstandaarden die compliance programma's verplichten, met regeldruk per sector of met het voorkomen van schandalen rond wetsovertreding die een stimulans zijn voor invoering van compliance programma's. In *figuur 29* is af te lezen dat 63% van de respondenten, die werkzaam zijn bij een financiële instelling, een compliance programma heeft. Ondanks een minimale stijging, blijft dit percentage opmerkelijk. Op grond van de Wet op het financieel toezicht ('Wft') zijn financiële instellingen verplicht tot het invoeren van een compliance programma. Ook meerdere geïnterviewde experts geven aan verrast te zijn door het 'lage' percentage compliance programma's binnen de financiële sector.

Naast een verschil per sector geven meerdere geïnterviewde experts aan dat het hebben van een compliance programma ook afhangt van de grootte van de organisatie. Een van de geïnterviewde experts vertelt: *"Grotere organisaties kunnen niet zonder compliance programma maar bij de middelgrote organisaties komt het minder voor"*.

Figuur 30 Compliance programma en Prevalentie traditionele financieel-economische criminaliteit

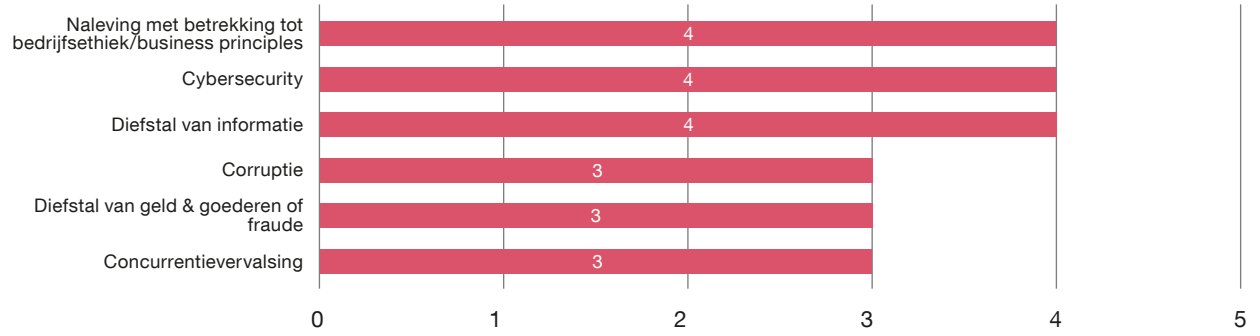


Compliance programma en financieel-economische criminaliteit

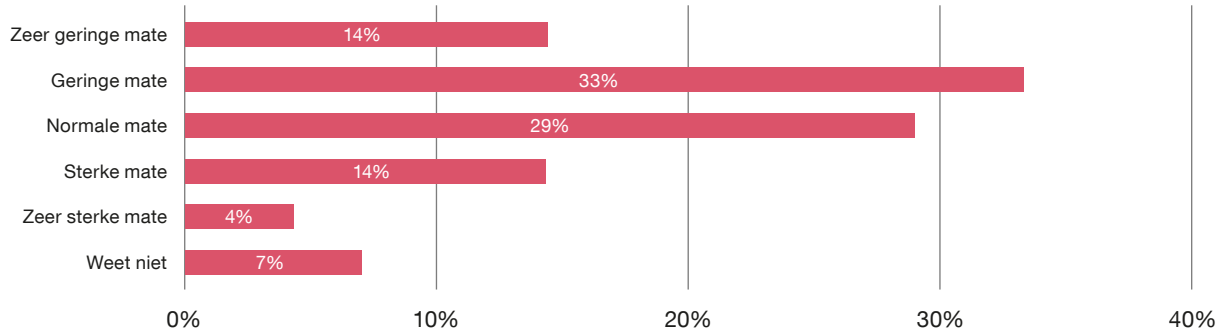
Figuur 30 laat de relatie zien tussen een compliance programma en de prevalentie van traditionele financieel-economische criminaliteit. Hieruit valt op te maken dat organisaties met een compliance programma vaker traditionele financieel-economische criminaliteit rapporteren in de survey. In eerste instantie trekt dit de effectiviteit van een compliance programma in twijfel, maar dit beeld is een voorbeeld van de eerder besproken controle-paradox. Wanneer beter gecontroleerd wordt op financieel-economische criminaliteit, zullen ook meer gevallen aan het licht komen.

Een compliance programma kan binnen een organisatie onder een andere naam zijn geïmplementeerd. Een 'bedrijfsintern milieuzorgsysteem' zoals te vinden bij veel bedrijven in de industriële sector is bijvoorbeeld een compliance systeem op het terrein van milieuwet- en regelgeving. Daardoor zou het kunnen dat niet alle medewerkers weten dat hun organisatie over een compliance-programma beschikt. Deze onduidelijkheid komt ook bij de interviews naar voren. Een van de geïnterviewde experts vertelt: *"Wij hebben een afdeling compliance. Daarbij monitoren wij op basis van voor ons relevante wetsgebieden, maar ik weet niet zeker of dit dan precies valt onder een 'compliance programma' zoals jullie dat bedoelen."*

Figuur 31 In hoeverre richt het compliance programma zich op de volgende zaken?



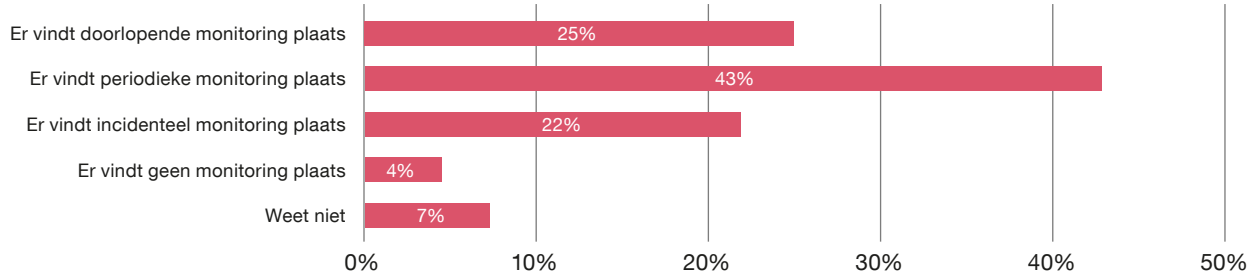
Figuur 32 In hoeverre worden de compliance vereisten door medewerkers als belastend ervaren?



Ook is in de survey gevraagd naar de invulling van het compliance-programma. Hierbij is gevraagd in hoeverre het programma zich richt op diefstal van geld of goederen of fraude, diefstal van informatie, corruptie, concurrentievervalsing, cybersecurity en bedrijfsethiek. Hierbij staat 1 voor 'in zeer geringe mate' en 5 voor 'zeer sterke mate'. Vervolgens is voor elk van de richtingen de mediaan uitgerekend, die weergegeven zijn in *figuur 31*. De mediaan ligt het hoogst voor de richtingen: diefstal van informatie, cybersecurity en naleving met betrekking tot de bedrijfsethiek/business principles. Volgens de respondenten richt het compliance programma zich meer op deze onderdelen dan op diefstal van geld of goederen of fraude, corruptie of concurrentievervalsing. Tijdens de interviews brengen meerdere experts naar voren dat de preventieve maatregelen binnen hun organisaties ook gericht zijn op het verhogen van de bewustwording ('awareness'). Zo stelt een van de experts: *"Je bereikt het meeste met awareness creëren en zorgen dat mensen melden als ze iets tegenkomen." "Met menselijk gedrag kan criminaliteit het beste voorkomen worden"*.

Vervolgens is aan de respondenten voorgelegd in hoeverre een compliance programma als belastend wordt ervaren. In *figuur 32* zijn de antwoorden op deze vraag te zien. De uitkomsten komen overeen met de editie uit 2019. Iets minder dan de helft van de respondenten met een compliance programma geeft aan dat de vereisten in (zeer) geringe mate belastend zijn. Desondanks geeft 18% van de respondenten aan een compliance programma in (zeer) sterke mate belastend te vinden.

Figuur 33 In hoeverre vindt er monitoring van het compliance programma plaats?



Een van de experts van de interviews zegt hierover: *"Elk jaar komt er iets meer bij, als je eenmaal begint aan compliance houdt het niet op"*. Anderzijds geeft deze expert wel aan dat er bepaalde voordelen zitten aan het inrichten van een compliance programma binnen de organisatie: *"Als autoriteiten meekijken word je anders behandeld als je een compliance programma hebt."* Ook geven meerdere experts in de interviews aan dat het hebben van een compliance programma van toegevoegde waarde is binnen hun organisatie.

Monitoring van het compliance programma

In 2021 werd in de media regelmatig geschreven over grote fraude- en witwasschandalen. Binnen de financiële sector heeft een organisatie met het Openbaar Ministerie getransigeerd voor 480 miljoen euro. In een eerdere en vergelijkbare zaak heeft het Openbaar Ministerie bij de transactie de voorwaarde van het instellen van een 'compliance monitor' opgenomen. Naast het invoeren en uitvoeren van een compliance programma, is het monitoren[5] van het compliance programma onderdeel uit gaan maken van integraal compliance management.

Om die reden is in de survey gevraagd in welke mate het compliance programma gemonitord wordt.

De uitkomsten zijn weergegeven in *figuur 33*. Hier is een afname in incidentele monitoring te zien. Dit is van 33% in 2019 gedaald naar 22% in deze editie. Desondanks geeft het merendeel van de respondenten aan dat hun compliance gemonitord wordt. ■

5 Het in de gaten houden van complexe processen en onderwerpen binnen compliance

7. Cultuur, corona en criminaliteit

Naast preventief beleid kan kwetsbaarheid voor financieel-economische criminaliteit samenhangen met de organisatiecultuur. Uit onderzoek blijkt dat dit in het bijzonder geldt voor de target- en bonuscultuur, de ethische bedrijfscultuur en de toon aan de top. Net als in de vorige editie hebben wij respondenten gevraagd naar deze aspecten van organisatiecultuur en hebben wij de samenhang met prevalentie van financieel-economische criminaliteit onderzocht. Organisatiecultuur hangt samen met de aard van de bedrijfsactiviteiten en de manier van werken binnen organisaties. Door de coronacrisis die in maart 2020 uitbrak, is de manier van werken bij veel organisaties drastisch gewijzigd, nu een groot aantal werknemers gedwongen was lange tijd thuis te werken. Een belangrijke vraag is welke effecten het thuiswerken heeft op de prevalentie van financieel-economische criminaliteit en de kwetsbaarheid van organisaties. Om die reden is in de Economic Crime Survey 2021 gevraagd naar de mate en de gevolgen van thuiswerken. Daarnaast zijn de gevolgen voor het voorkomen van financieel-economische criminaliteit onderzocht.

Target- en bonuscultuur

Eerst kijken we of een target- en bonuscultuur invloed heeft op onethisch werknemersgedrag. Op die manier kan beargumenteerd worden of dit een mogelijke bijdrage levert aan de totstandkoming van financieel-economische criminaliteit.

In onze survey is de respondenten een viertal vragen gesteld met betrekking tot een target- en bonuscultuur. Zo is bijvoorbeeld gevraagd naar het belang van bijzondere beloningen (zoals bonussen) en het behalen van targets. Maar ook is gevraagd naar de mate waarin de salarissen bestaan uit bijzondere beloningen. Daarbij kon de keuze gemaakt worden tussen vijf verschillende antwoordmogelijkheden, oplopend van 1 (helemaal mee oneens) tot 5 (helemaal mee eens). Op de vraag over het belang van bonussen in een organisatie, is per sector verschillend geantwoord. Het overzicht hiervan is te zien in *figuur 34*. Uit dit figuur blijkt dat de sectoren ‘bosbouw, landbouw, visserij en mijnbouw’ en ‘industrie’ de hoogste score laten zien op deze vraag.

Stellingen met betrekking tot een target- en bonuscultuur

1. Een belangrijk deel van de salarissen in onze organisatie bestaat uit bijzondere beloningen (vb. bonussen).
2. Onze organisatie verbindt voor medewerkers grote belangen aan het behalen van targets.
3. Binnen onze organisatie spelen bijzondere beloningen (zoals bonussen) een belangrijke rol.
4. Binnen onze organisatie hecht men grote waarde aan het behalen van targets.

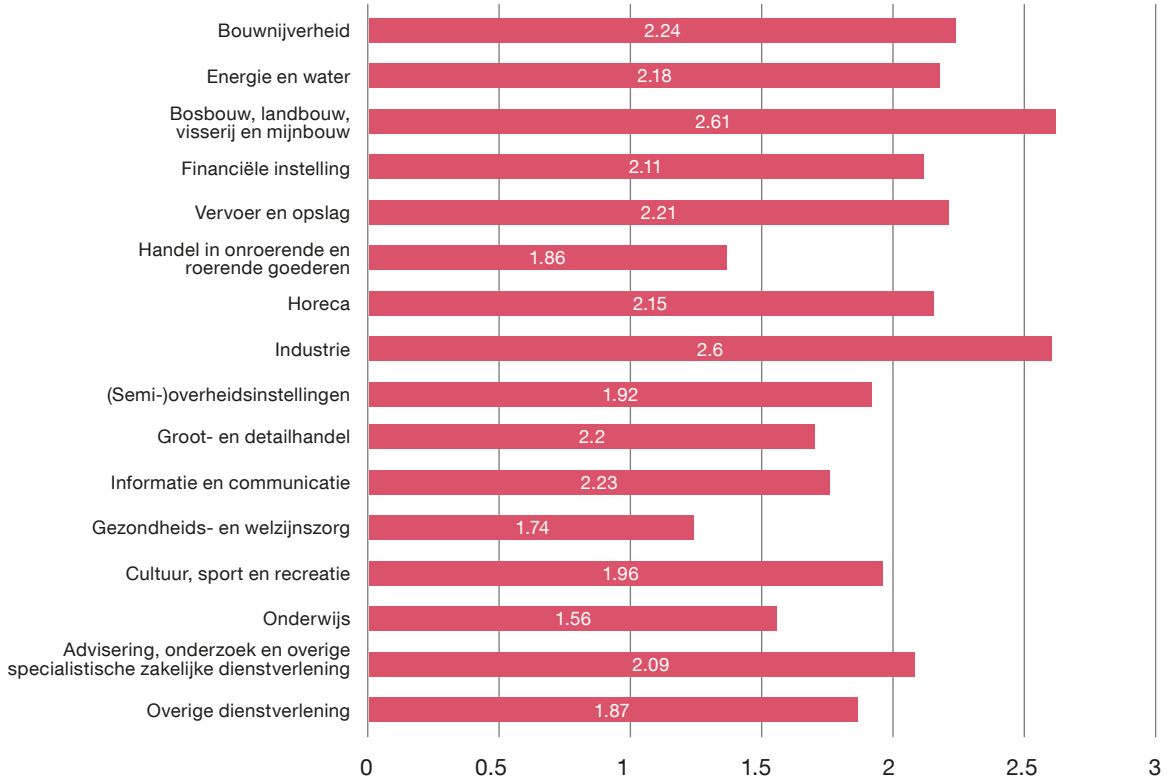
Dat betekent dat er binnen deze sectoren relatief gezien in grotere mate een bonuscultuur heerst. De sectoren die hier het minste belang aan hechten zijn ‘onderwijs’ en ‘gezondheids- en welzijnszorg’. De resultaten zijn weergegeven in de paragraaf ‘organisatiecultuur en financieel-economische criminaliteit’.

Ethische bedrijfscultuur

De ethische bedrijfscultuur wordt gevormd door de gedeelde morele opvattingen van leden van de organisatie. De ethische bedrijfscultuur is daarbij een onderdeel van de bedrijfscultuur en organisatiecultuur die het ethisch gedrag van de organisatie voorspelt (Key, 1999). Volgens onderzoekers kan verondersteld worden dat organisaties met een onethische bedrijfscultuur zich eerder schuldig zullen maken aan diverse vormen van regelovertreding. Aan de andere kant zou een ethische bedrijfscultuur zorgen voor een hogere drempel bij medewerkers van de organisatie om regelovertreding te begaan. Op die manier kunnen leden van een organisatie met een ethische bedrijfscultuur worden weerhouden van regelovertreding of ander onethisch gedrag (Denkers, Peeters & Huisman, 2013).

Om uitspraken te kunnen doen over de ethische bedrijfscultuur bij organisaties in Nederland, is de respondenten in de Economic Crime Survey gevraagd uitspraken te doen over de ethische bedrijfscultuur in hun organisatie. Op die manier hebben de respondenten antwoord gegeven op zes verschillende stellingen met betrekking tot de ethische bedrijfscultuur van hun organisatie. Hierbij varieerden de antwoordmogelijkheden

Figuur 34 Bonuscultuur per sector



opnieuw van 1 (helemaal mee oneens) tot 5 (helemaal mee eens). Van deze zes stellingen is een samengevoegde variabele gemaakt, zodat de gemiddelden van de resultaten op de stellingen met elkaar vergeleken kunnen worden. Hoe hoger het gemiddelde cijfer is, hoe ethischer de bedrijfscultuur van de organisatie is. De resultaten zijn weergegeven in de paragraaf 'organisatiecultuur en financieel-economische criminaliteit'.

Stellingen met betrekking tot een ethische bedrijfscultuur

1. Medewerkers binnen mijn organisatie houden zich aan de regels en voorschriften.
2. Medewerkers binnen mijn organisatie laten zich vooral leiden door hun eigen belang.
3. In mijn organisatie spelen ethische principes een belangrijke rol bij het nemen van beslissingen.
4. In mijn organisatie is het vooral 'ieder voor zich'.
5. Het welzijn van de medewerkers staat centraal in onze organisatie.
6. Mensen in onze organisatie hebben een sterk verantwoordelijkheidsgevoel ten opzichte van de maatschappij en de mensheid.

Toon aan de top

Een juiste toon aan de top is erg belangrijk voor het bewerkstelligen van een ethische bedrijfscultuur. Volgens Gunz en Thorne (2015) komt de toon aan de top overeen met een ethische omgeving binnen een organisatie, die is gecreëerd door het leiderschap van de organisatie. In dit onderzoek wordt toon aan de top gezien als een verticale verbinding tussen hoger management en de werknemers, waarbij het hoger management zorgt voor de mate van ethische bedrijfscultuur binnen de organisatie. Daarbij wordt in onderzoeken gesteld dat het management van de organisatie ervoor kan zorgen dat medewerkers zich juist wel of niet aan de regels houden. Zo kan het management van de organisatie bepaalde regels binnen de organisatie opstellen waar alle medewerkers zich aan moeten houden. Daarbij kan bijvoorbeeld een bepaald intern sanctiesysteem gehanteerd

worden. Ook kunnen de medewerkers worden voorzien van een ethisch trainingsprogramma, wat volgens Gunz en Thorne (2015) een bijdrage levert aan een ethische bedrijfscultuur. Om uitspraken te kunnen doen over de toon aan de top bij organisaties in Nederland, zijn de respondenten in de Economic Crime survey vijf stellingen voorgelegd met betrekking tot toon aan de top. Daarbij konden de respondenten opnieuw kiezen uit vijf verschillende antwoordmogelijkheden, variërend van 1 (helemaal mee oneens) tot 5 (helemaal mee eens). Ook van deze vijf stellingen is een samengevoegde variabele gemaakt, waarbij de gemiddelden berekend zijn. De gemiddelden geven daarbij de algemene score op toon aan de top. In de volgende alinea zijn de resultaten hiervan weergegeven.

Stellingen met betrekking tot de toon aan de top

1. is te vertrouwen.
2. neemt beslissingen op basis van wat juist is.
3. geeft het goede voorbeeld m.b.t. ethisch handelen.
4. definieert succes niet enkel op basis van resultaten, maar ook hoe deze tot stand zijn gekomen.
5. onderneemt actie wanneer medewerkers ethische normen overschrijden.

Organisatiecultuur en financieel-economische criminaliteit

We hebben onderzocht of de drie aspecten van organisatiecultuur samenhangen met de financieel-economische criminaliteit waarmee organisaties in aanraking komen. Voor bonus- en targetcultuur, ethische bedrijfscultuur en toon aan de top zijn aparte Pearson correlaties[6] uitgevoerd. Dit is gedaan door de stellingen

per variabele samen te voegen tot een nieuwe variabele, waarbij het gemiddelde antwoord op de stellingen te zien is. Voor bonus- en targetcultuur heeft dit een zwakke positieve correlatie opgeleverd. Dat betekent dat respondenten die werkzaam zijn in een organisatie met een hoge mate van een bonus- en targetcultuur, vaker aangeven dat de organisatie in aanraking is gekomen met financieel-economische criminaliteit.

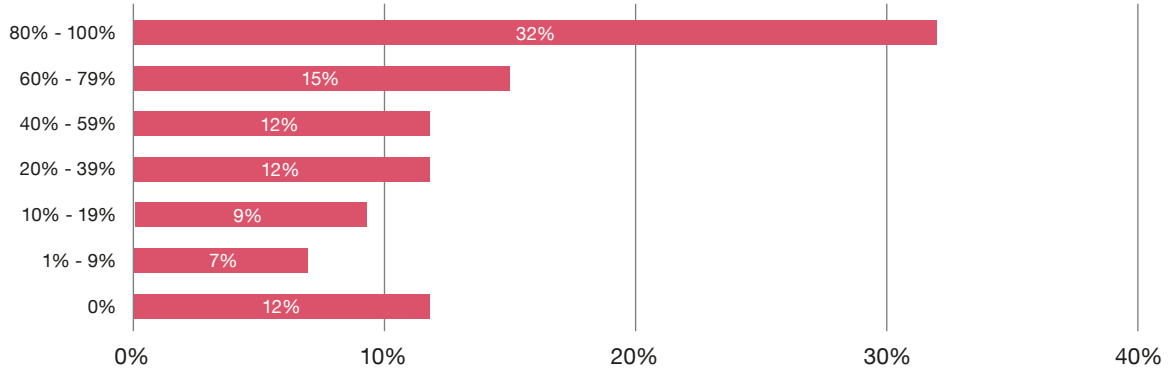
Voor ethische bedrijfscultuur en toon aan de top heeft dit een zwakke negatieve correlatie opgeleverd. Dat betekent dat respondenten die werkzaam zijn in organisaties met een hogere mate van ethische bedrijfscultuur of toon aan de top, minder vaak aangeven dat de organisatie in aanraking is gekomen met financieel-economische criminaliteit. Deze bevindingen zijn in lijn met de vorige editie van de Economic Crime Survey, aangezien de correlaties toen vergelijkbare uitkomsten lieten zien.

6 Een Pearson correlatie meet de samenhang tussen twee continue variabelen uit in een getal tussen -1 en 1. Naarmate dit getal hoger is, is de samenhang tussen de variabelen sterker.

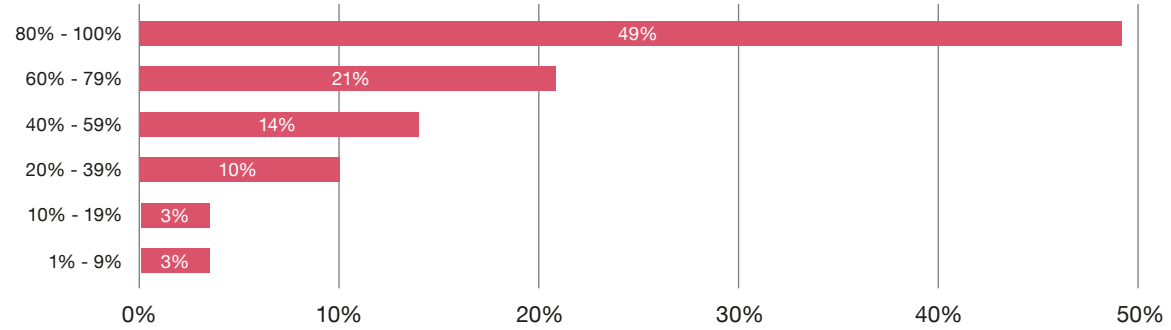
Coronacrisis en thuiswerken

Een ingrijpende gebeurtenis die de afgelopen twee jaar heeft plaatsgevonden is uiteraard de uitbraak van Covid-19. Deze pandemie heeft ervoor gezorgd dat veel organisaties hun werknemers opleggen vanuit huis te werken om de verspreiding van dit snel om zich heen grijpende virus tegen te gaan. Om deze reden is dit jaar in de Economic Crime Survey gevraagd hoeveel procent van de medewerkers thuiswerkt gedurende de pandemie en hoeveel procent van de tijd dat uiteindelijk is. In *figuur 35* is af te lezen dat met 32% de grootste categorie wordt gevormd door organisaties van wie 80%-100% van de medewerkers thuiswerken. Dit is met afstand de grootste groep. Wanneer gekeken wordt naar de totale werktijd dat thuis wordt gewerkt is een vergelijkbaar beeld te zien. 49% van de respondenten die thuiswerkt doet dat 80%-100% van hun totale werktijd. 21% van de desbetreffende personen werkt 60%-79% van de totale werktijd thuis. Het overzicht hiervan is te zien in *figuur 36*. Deze resultaten liggen in de lijn der verwachting gezien veel organisaties door de pandemie thuiswerken hebben verplicht en ook de overheid heeft aanbevolen om zo veel mogelijk thuis te werken.

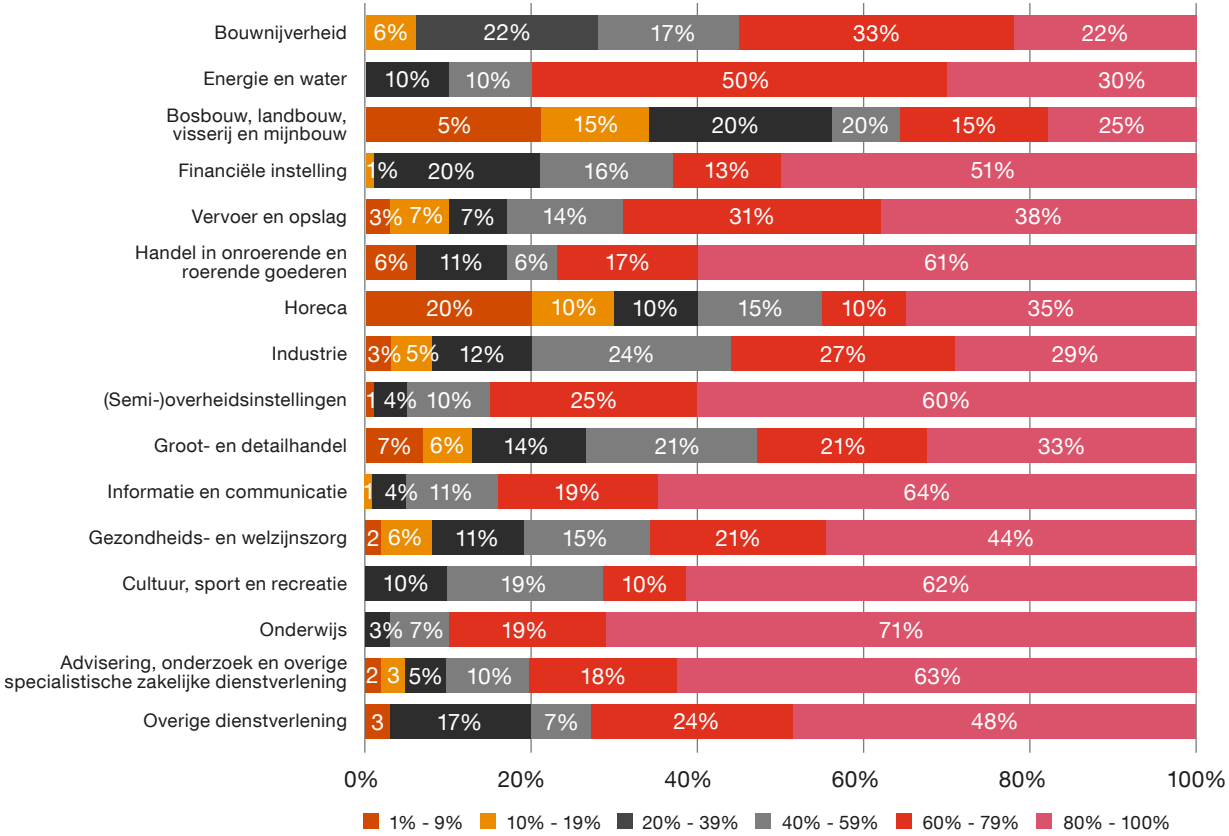
Figuur 35 Percentage medewerkers dat thuiswerkt tijdens de coronapandemie



Figuur 36 Percentage van de totale werktijd dat thuis wordt gewerkt



Figuur 37 Percentage thuiswerkers per sector



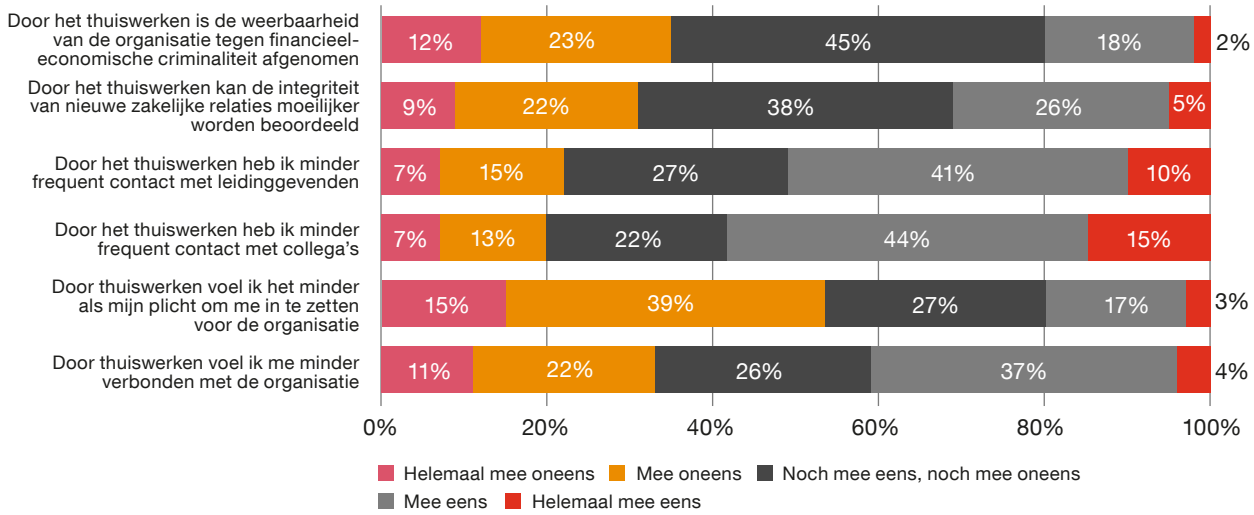
De afgelopen twee jaar is thuiswerken door de coronacrisis plotseling de standaard geworden. In bepaalde sectoren wordt meer thuisgewerkt dan in andere sectoren. Hierdoor kan de prevalentie in bepaalde sectoren sterker door thuiswerken zijn beïnvloed dan in andere sectoren. In *figuur 37* is af te lezen dat 71% van de respondenten uit de onderwijssector en 63% van de respondenten uit de sector advisering, onderzoek en overige specialistische zakelijke dienstverlening aangeven dat 80%-100% van hun werknemers thuiswerken. De laagste relatieve cijfers zijn gevonden voor de sectoren: bouwnijverheid (22%) en bosbouw, landbouw, visserij en mijnbouw (25%).

Thuiswerken en weerbaarheid

Om de invloed van de coronacrisis verder in kaart te brengen zijn verschillende vragen gesteld over de impact van thuiswerken voor werknemers en hun organisaties. Ten eerste is aan de respondenten voorgelegd of door het thuiswerken de weerbaarheid van de organisatie tegen financieel-economische criminaliteit is afgenomen. Uit *figuur 38* blijkt 35% van de respondenten vindt dat de weerbaarheid niet is afgenomen en 20% vindt dat de weerbaarheid wel is afgenomen. Daarnaast is gevraagd of de beoordeling van de integriteit van nieuwe zakelijke relaties moeilijker kan worden beoordeeld door thuiswerken. De antwoordcategorieën ‘eens’ en ‘oneens’ zijn voor deze stelling evenredig verdeeld in groepen van 31%.

Vervolgens zijn vragen gesteld over het thuiswerken en contact met leidinggevenden en collega’s. Achterliggende gedachte is dat formele en informele controle gelegenheid tot financieel-economische criminaliteit wegnemen. Afname van controle is dan een risicofactor. Uit de antwoorden blijkt dat respondenten minder frequent contact hebben met zowel collega’s als leidinggevenden. 51% geeft aan minder

Figuur 38 In hoeverre bent u het eens met de volgende stellingen?



contact te hebben met leidinggevenden en 49% geeft aan minder contact te hebben met collega's. Daarnaast geeft 41% van de respondenten aan zich door het thuiswerken minder verbonden te voelen met de organisatie. Ook een verminderde gebondenheid met de organisatie kan een rem op betrokkenheid bij financieel-economische criminaliteit wegnemen. Ook al voelt 41% van de respondenten zich minder verbonden met de organisatie, slechts 20% voelt ook minder de plicht om zich in te zetten voor de werkgever.

Thuiswerken en prevalentie van financieel-economische criminaliteit

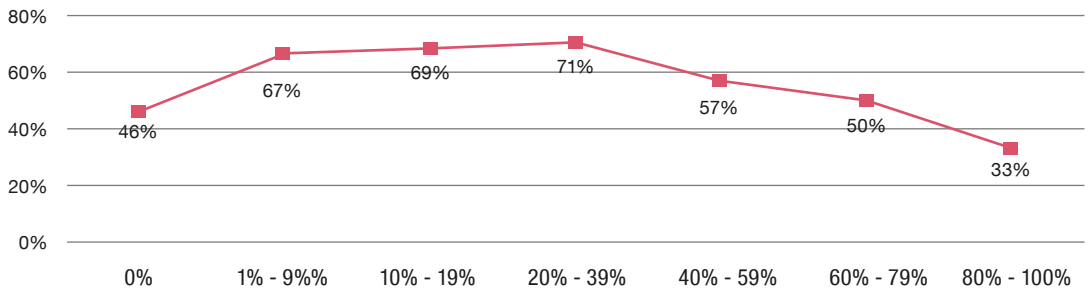
Tenslotte zijn de mogelijke gevolgen van het thuiswerken door de coronacrisis voor de financieel-economische criminaliteit bestudeerd. Daartoe is de correlatie[7] tussen de bovenstaande stellingen over thuiswerken en de prevalentie traditionele financieel-economische criminaliteit en cybercriminaliteit onderzocht. Hierbij zijn voor alle stellingen en vormen van financieel-economische criminaliteit positieve zwakke significante verbanden gevonden. Indien een respondent aangeeft dat de organisatie in aanraking is gekomen met financieel-economische criminaliteit, zijn ze het meer eens met de stellingen uit figuur 38.[8]

7 Door middel van een Spearman's Rho correlatie kan de mate van samenhang uitgedrukt worden tussen dichitome en ordinale variabele. Deze samenhang wordt uitgedrukt in een getal tussen -1 en 1. Hoe dichter het getal bij -1 of 1 ligt, hoe sterker de samenhang tussen de variabelen is.
8 Hierbij dient echter wel vermeld te worden dat de stellingen: 'Door het thuiswerken voelen medewerkers binnen mijn organisatie zich minder verbonden met de organisatie' en 'Door het thuiswerken is de weerbaarheid van de organisatie tegen financieel-economische criminaliteit afgenomen' enkel significant zijn voor cybercriminaliteit een alpha van 10%. Dit betekent dat de kans op een significant onbetrouwbare uitkomst van de toets maximaal 10% is.

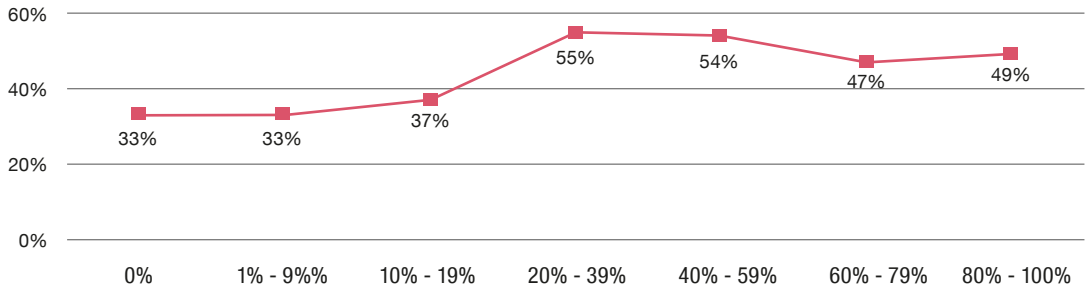
Uit meerdere interviews blijkt dat de experts verwachten dat thuiswerken invloed heeft gehad op de prevalentie van traditionele financieel economische criminaliteit, maar het verschilt of men een daling of stijging verwacht. Een van de geïnterviewde experts stelt: *"Hierdoor is er minder informeel toezicht op andere werknemers, waardoor diefstal van geld, goederen of informatie eerder onder de radar zal blijven en er daardoor een dalende trend zichtbaar is"*. Daarnaast geven geïnterviewde experts aan dat diefstal van goederen door gesloten kantoren ook lastiger te plegen is.
"Ik kan mij voorstellen dat in corona tijd, fysieke daden zoals stelen lastiger zijn omdat je niet op kantoor bent."
Dit sluit aan bij de bevindingen uit figuur 1, waar te zien is dat diefstal van geld of fraude is afgenomen ten opzichte van de vorige editie.

Daarnaast is het percentage thuiswerkers binnen de organisatie afgezet tegen de prevalentie van alle vormen van traditionele financieel-economische criminaliteit en cybercriminaliteit. Hieruit is bij (nagenoeg) alle vormen een vergelijkbaar bergparabool te herkennen, zoals in *figuur 39*. Dit houdt in dat de prevalentie het laagst ligt wanneer veel medewerkers of geen medewerkers thuiswerken. Oftewel, wanneer bij organisaties 1% t/m 39% van de medewerkers thuiswerken ligt de prevalentie het hoogst. Met andere woorden: bij de toename van het aantal thuiswerkers neemt de prevalentie van financieel-economische criminaliteit eerst toe, maar vanaf een bepaald niveau van thuiswerken neemt die prevalent ook weer af. De geïnterviewde experts vinden het lastig dit patroon te verklaren. Gegeven verklaringen zijn vaak sectorspecifiek. Zo suggereert een expert uit de industriële sector die inschat dat 20-39% van de werknemers thuiswerkt dat dit patroon voor zijn organisatie verklaard zou kunnen worden doordat op de productielocaties met lagere bezetting wordt gewerkt. Er zijn dus nog wel werknemers die goederen kunnen stelen, maar er zijn minder collega's die hen daarop zouden kunnen betrappen.

Figuur 39 Percentage thuiswerkers binnen de organisatie en de prevalentie van diefstal van geld of goederen of fraude



Figuur 40 Percentage thuiswerkers binnen de organisatie en de prevalentie van phishing



Uit *figuur 40* blijkt dat phishing een andere trend laat zien wanneer de prevalentie wordt afgezet tegen het percentage thuiswerkers binnen de organisatie. Wederom zijn voor de lagere percentage groepen de laagste relatieve prevalentiecijfers te vinden. Vanaf de groep van 20%-39% vindt er echter geen daling plaats, maar

blijven de prevalentiecijfers schommelen rond de 50%. Daarnaast vindt voor cybercriminaliteit een minder harde daling plaats. Kortom de prevalentiecijfers voor de vormen van cybercriminaliteit dalen minder hard wanneer meer medewerkers binnen een organisatie thuiswerken.

Uit een van de interviews met een expert van de politie komt naar voren dat dit ook te maken kan hebben met de mate van ondersteuning van thuiswerkers door organisatie. Hierbij geeft de expert aan dat als je ondersteund wordt in het thuiswerken door een grote organisatie, je hierbij vaak ook beter beschermd bent. Bij grote organisaties zorgt de IT-afdeling ervoor dat de thuiswerkers op beveiligde apparatuur van de zaak werken. Dit in tegenstelling tot kleine organisaties waarbij de mensen thuis moet werken op privé laptops waarbij meer risico ontstaat. Een andere expert geeft aan dat er 'maar zoveel' phishing mails worden verstuurd en dat dit maximum al vanaf een bepaalde hoeveelheid thuiswerktijd wordt ontvangen.

Daarnaast zijn voor de variabelen 'percentage thuiswerkers binnen een organisatie' en 'thuiswerktijd' correlaties berekend voor de verschillende vormen van financieel-economische criminaliteit. Dit heeft een zwak negatief verband opgeleverd tussen diefstal van geld of goederen of fraude en het percentage thuiswerkers binnen de organisatie (-0.063). Dit houdt in dat naarmate organisaties slachtoffer zijn geworden van diefstal van geld of goederen of fraude minder werknemers thuiswerken. Deze conclusie lijkt af te wijken van figuur 39, maar het gaat hier om een correlatie. Een zwak positief verband is gevonden tussen de prevalentie van phishing (0.059) en social engineering (0.063) enerzijds en het percentage thuiswerkers binnen een organisatie anderzijds.

Indien organisaties slachtoffer zijn geworden van phishing of social engineering, meer mensen thuiswerken.
Wel moet hierbij vermeld worden dat deze resultaten alleen significant zijn op een alpha van 10%. Zoals eerder opgemerkt betekent dit dat de kans op een significant onbetrouwbare uitkomst van de toets maximaal 10% is.

Aangezien voor de meeste vormen van financieel-economische criminaliteit geen verband is vastgesteld en de drie verbanden die wel significant zijn, uitermate zwak zijn, is gekeken naar verbanden tussen het percentage thuiswerkers en de 'totale' prevalentie voor traditionele financieel-economische criminaliteit en cybercriminaliteit. Voor cybercriminaliteit leverde dit een positief zwak verband op tussen de prevalentie en het percentage medewerkers dat thuiswerkt (0.102).

Indien organisaties slachtoffer zijn geworden van cybercriminaliteit, werken meer medewerkers thuis.
Voor traditionele financieel-economische criminaliteit werden twee zwakke negatieve verbanden gevonden voor prevalentie traditionele financieel-economische criminaliteit enerzijds en het percentage medewerkers dat thuiswerkt (-0.182) en het percentage thuiswerk tijd (-0.197) anderzijds. Hieruit kan geconcludeerd worden dat indien een organisatie slachtoffer is geworden van traditionele financieel-economische criminaliteit, minder medewerkers thuiswerken of minder tijd daadwerkelijk thuisgewerkt wordt. ■

Methodologische verantwoording

In dit hoofdstuk zullen de gebruikte onderzoeksmethoden worden besproken. Daarbij zullen methodologische begrippen als ‘validiteit’, ‘betrouwbaarheid’ en ‘triangulatie’ uitgelegd worden. Daarnaast wordt gewezen op het belang van deze begrippen voor wetenschappelijk onderzoek. Ook zal worden uitgelegd hoe de vragenlijst tot stand gekomen is en hoe de respondenten zijn benaderd. Daarnaast zal verder uiteengezet worden hoe de experts uit de interviews benaderd zijn en waarom er voor deze experts is gekozen.

Validiteit, triangulatie en betrouwbaarheid

Om de kwaliteit van de resultaten uit dit rapport te waarborgen, zijn de methodologische begrippen validiteit en betrouwbaarheid in acht genomen. De validiteit is de mate waarin het onderzoek meet wat het beoogt te meten (Bijleveld, 2013). Om de validiteit in acht te nemen is een definitielijst toegevoegd aan de vragenlijst. Hiermee is ervoor gezorgd dat de respondenten de begrippen uit de vragenlijst begrijpen. Op die manier meten de vragen in de vragenlijst wat zij beogen te meten. Zo is in de Economic Crime Survey van 2019 gebleken dat bepaalde antwoordopties binnen cybercriminaliteit niet werden herkend door de respondenten waardoor de antwoordcategorieën in deze editie zijn aangepast. Hierbij zijn voor cybercriminaliteit de antwoordopties uit 2019, zijnde ‘error’, ‘sociale cybercrime’, ‘fysieke cybercrime’ en ‘omgevingsgerelateerde cybercriminaliteit’ vervangen door ‘DDoS’, ‘ransomware’, ‘phishing’ en ‘social engineering’. Op deze manier is getracht het onderzoek meer valide te maken door de invoering van de vernieuwde antwoordcategorieën. Wel is het moeilijk om er middels van de vragenlijst zeker van te zijn dat de ondervonden empirische verbanden tevens causale verbanden zijn. Daarom is in dit onderzoek gekozen voor triangulatie. Triangulatie is het combineren van verschillende theorieën, methoden en/of databronnen om de onderzoeksvragen van een onderzoek te kunnen beantwoorden en meer inzicht in een onderwerp te verkrijgen (Oates, 2006). Voor de Economic Crime Survey 2021 zijn net als in de voorgaande editie vier verschillende bronnen gebruikt: een vragenlijst, expertinterviews, de praktijkkennis van PwC en (wetenschappelijke) literatuur. Op die manier kunnen de ondervonden resultaten uit de vragenlijst ondersteund worden door andere onderzoeksmethoden, bijvoorbeeld door de expertinterviews. Tot slot is de betrouwbaarheid in acht de genomen. De betrouwbaarheid is de nauwkeurigheid waarmee is gemeten (Bijleveld, 2013). In dit onderzoek is de betrouwbaarheid in acht genomen doordat de vragenlijst waarmee de data is verzameld, opgesteld is in overeenstemming met de VU en afgenomen is door onderzoeksbureau FlyCatcher. Flycatcher voldoet aan de ISO-kwaliteitseisen. Deze data is vervolgens geanalyseerd door middel van het statistiekprogramma SPSS.

Vragenlijst

Voor het uitzetten van de vragenlijst is gebruik gemaakt van onderzoeksbureau Flycatcher. Dit bureau voldoet aan de ISO-kwaliteitseisen voor sociaalwetenschappelijk onderzoek, markt-, en opinieonderzoek. Het Flycatcher panel bestaat uit meer dan 10.000 personen die zich via ‘double-active-opt-in’ vrijwillig en actief bereid hebben verklaard om deel te nemen aan online onderzoeken. Bij het openen van de gepersonaliseerde link uit de e-mail, wordt een verificatievraag gesteld en wordt gevraagd of de achtergrondgegevens nog actueel zijn.

Voor dit onderzoek zijn de respondenten die in 2019 hebben deelgenomen aan de Economic Crime Survey opnieuw uitgenodigd[9]. De onderzoeksgroep is geselecteerd uit het Flycatcher panel. In totaal hebben 5702 panelleden van Flycatcher een uitnodiging gekregen.

9 Het is niet duidelijk hoeveel respondenten opnieuw hebben deelgenomen en hoeveel respondenten er nieuw zijn in deze editie.

In totaal zijn er 3373 vragenlijsten volledig ingevuld waarbij 875 respondenten voldeden aan de selectievraag en binnen de doelgroep vielen. Deze selectievraag hield in dat respondenten werd gevraagd of zij uit hoofde van hun functie belast zijn met het in kaart brengen, voorkomen of aanpakken van vijf verschillende vormen van financieel-economische criminaliteit. Hieruit blijkt dat 70% van de respondenten zich bezighoudt met de bestrijding van diefstal van geld of goederen of fraude, 47% met corruptie, 67% met diefstal van informatie en 38% met concurrentievervalsing. Deze selectievraag heeft ertoe geleid dat de respondenten alleen toegang kregen tot het vervolg van de survey indien ze hadden aangegeven belast te zijn met het in kaart brengen, voorkomen of aanpakken van financieel-economische criminaliteit. Verder blijkt uit analyse dat voor cybercriminaliteit 52% van de respondenten deskundige is op gebied van hacking, 50% van malware, 34% DDoS, 53% van phishing, 35% van social engineering, 55% van misbruik en 45% van ransomware.

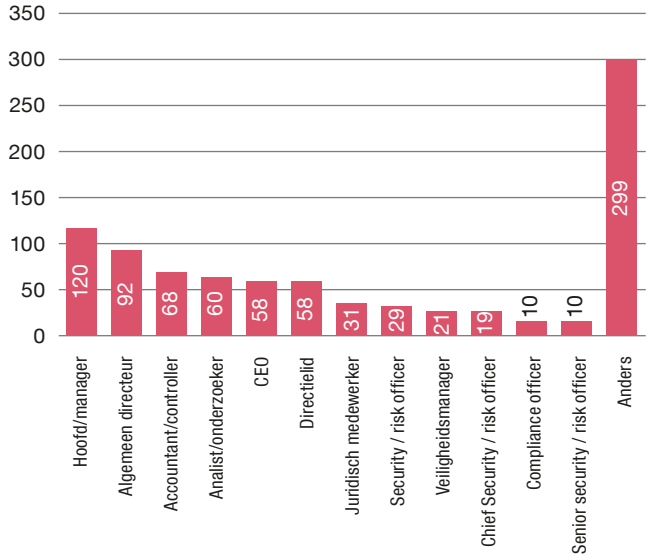
Vragenlijst - Respondenten

Tevens is gevraagd hoe lang de respondenten ten tijde van de vragenlijst in hun huidige functie werken, gemiddeld kwam hier negen jaar uit. De respondenten is gevraagd wat hun functie is en daarbij zijn twaalf verschillende opties gegeven of konden de respondenten hun eigen functie beschrijven. De respondenten kozen in 66% van de gevallen voor een van voorgelegde opties. 328 respondenten gaven aan een leidinggevende functie te bekleden, waaronder de antwoordopties CEO, manager, directielid of algemeen directeur vielen. 68 respondenten gaven aan accountant/controller te zijn, 60 analist/onderzoeker, 31 juridisch medewerker, 29 security/ risk officer, 10 compliance officer en 21 veiligheidsmanager.

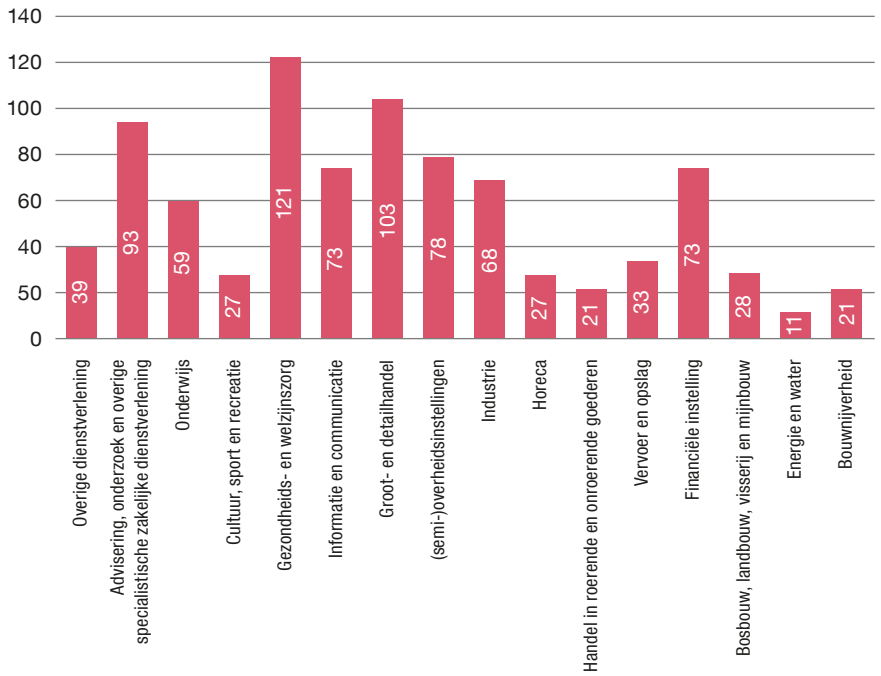
Als laatste gaven 299 respondenten aan iets anders te doen dan de opgegeven opties. Zie *figuur 41* voor een overzicht van de functies van de respondenten.

Daarnaast is gevraagd in welke sector de respondent werkzaam is. De verschillende sectoren zijn gebaseerd op de indeling van het Centraal Bureau voor de statistiek ('CBS') en komen overeen met de Economic Crime Survey van 2019. Hierbij was er voor de respondenten keuze uit 19 sectoren. In de vorige editie is een grenswaarde aangehouden van minimaal 20 respondenten om de sectoren in beeld te brengen. In de huidige editie is er echter sprake van een grote spreiding van respondenten onder de verschillende sectoren. Derhalve is ervoor gekozen om de grenswaarde in deze editie te verlagen naar 11 respondenten. Dit had te maken met het lage aantal respondenten in de sector energie en water. Een lagere grenswaarde is mogelijk, omdat dit een beter beschrijvend beeld geeft van de sectoren en we geen statistische toetsen uitvoeren met de verschillende sectoren. In figuur 41 valt een redelijke spreiding van respondenten in de verschillende sectoren waar te nemen.

Figuur 41 Functies binnen de organisaties



Figuur 42 Aantal respondenten per sector



De vragen

Achtergrondkenmerken

De vragenlijst begint met de vraag of de respondenten uit hoofde van hun functie belast zijn met het in kaart brengen, voorkomen of aanpakken van de vijf genoemde vormen van financieel-economische criminaliteit. Vervolgens zijn vragen gesteld over de functie van de respondent en hoe lang de respondenten werkzaam zijn binnen hun huidige functie. Daarna zijn vragen gesteld over de organisatie. Te denken valt aan het aantal personeelsleden en de sector. Een onderdeel wat hierbij dit jaar nieuw is, is de vraag over de invloed van de Brexit op het frauderisico.

Prevalentie en schade

De respondenten is gevraagd hoe vaak de organisatie de afgelopen 2 jaar in aanraking is gekomen met financieel-economische criminaliteit. Wanneer zij aangeven dat de organisatie daarmee in aanraking is gekomen, worden meer specifieke vervolgvragen gesteld.
Daarna wordt cybercriminaliteit op een meer uitgebreide manier dan twee jaar geleden uitgevraagd. Voor zowel traditionele financieel-economische criminaliteit als cybercriminaliteit is naar het meest recente en meest ernstige delict gevraagd. Er zijn vragen gesteld over de dader, slachtoffers, afhandeling en schade.

Detectie en preventie

Aan de respondenten is gevraagd naar een eventueel compliance programma, trainingen en andere maatregelen om financieel-economische criminaliteit tegen te gaan. Daarnaast zijn dit jaar voor het eerst vragen gesteld over in hoeverre gebruik wordt gemaakt van threat intelligence en incident response bij de detectie van financieel-economische criminaliteit.

Organisatiecultuur

Ook zijn de respondenten vragen voorgelegd over de cultuur van de organisatie waar de respondent werkzaam is. Meer specifiek is gevraagd naar bijzondere beloningen en ethiek. De vragen over ethische bedrijfscultuur zijn ontleend aan het proefschrift van Gorsira (2018).

Corona en thuiswerken

Tot slot is een nieuw onderdeel toegevoegd waarin de invloed van het thuiswerken is besproken. Hierbij is gevraagd in welke mate men thuis werkt en zijn er een aantal stellingen voorgelegd over de binding met de eigen organisatie en zijn diepgaande analyses uitgevoerd op de uitkomsten.

Tabel 1 Selectievraag “Bent u uit hoofde van uw functie belast met … ”

	In kaart brengen	Voorkomen	Aanpakken
Diefstal van geld of goederen of fraude	265	429	232
Corruptie	185	278	147
Diefstal van informatie	233	426	205
Concurrentievervalsing	139	220	113
Hacking	162	331	168
Malware	164	306	164
Denial of service	130	189	116
Phishing	181	322	164
Social-engineering	132	197	115
Misbruik	195	331	186
Ransomware	160	267	154

De expertinterviews

Selectie en benadering experts

Dit jaar is er invulling gegeven aan het kwalitatieve onderdeel van het onderzoek door tien experts te interviewen. Deze experts houden zich met hun dagelijkse werkzaamheden bezighouden met financieel-economische criminaliteit. Deze experts zijn relaties van PwC's Forensic Services en zijn door de betreffende contactpersoon van PwC benaderd.

Er is getracht om experts uit verschillende sectoren te spreken om zo een breed beeld te krijgen van de ervaringen in de praktijk. Ook is er bewust voor gekozen om een expert te interviewen uit de sector energie en water omdat de opkomst hiervan in de survey laag was. Ook was er een expert die op basis van werkervaring uit het verleden over meerdere sectoren uitspraken kon doen.

Tabel 2 Experts per sector

Expert	Sector
1	Gezondheids- en welzijnszorg
2	Financiële instelling
3	Energie en water
4	Onderwijs
5	Bouwnijverheid
6	Vervoer en opslag/Industrie
7	Politie
8	Politie
9	Openbaar Ministerie
10	Openbaar Ministerie

De tien experts die hebben toegezegd mee te willen werken aan het onderzoek zijn vervolgens door PwC per e-mail benaderd voor een afspraak. Alle interviews zijn middels videogesprekken op afstand afgenomen en namen ongeveer een uur in beslag. De gesprekken hebben plaatsgevonden tussen 28 april en 3 juni 2021.

Interview structuur

Er is gekozen om semigestructureerde interviews te houden. De experts hebben tijdens het gesprek de meest opvallende resultaten voorgelegd gekregen en zijn gevraagd hierop te reageren. De interviews zijn dus geen herhaling van de vragenlijst geweest, maar waren bedoeld om de uitkomsten van de vragenlijst te duiden. Het voordeel van deze interviews is dat deze methode de mogelijkheid biedt op een open en contextuele manier informatie te verzamelen (Bijleveld, 2013).

Daarnaast faciliteert deze onderzoeksmethode het doorvragen naar het individuele perspectief en de reactie van de persoon. Met de interviews is getracht meer duiding te geven aan de resultaten uit de survey.

Met toestemming van de experts zijn de interviews opgenomen en is er een gespreksverslag opgesteld. De (anonieme) quotes die in het rapport staan zijn voorgelegd aan de respondenten en met hun toestemming gebruikt. ■

Literatuurlijst

Bijleveld, C.C.J.H. (2013). Methoden en technieken van onderzoek in de criminologie. Den Haag, Nederland: Boom uitgevers.

Bleker - van Eyk, S.C. (2020). Algoritme: de oplossing of Mammon? Tijdschrift voor compliance. 142-146.

Bullée, J.W.H., Montoya, L., Pieters, W., Junger, M. & Hartel, P. (2018). On the anatomy of social engineering attacks. A literature-based dissection of successful attack. Journal of Investigative Psychology and Offender Profiling, 15(1), 20-45.

Dehghantanha, A., Conti, M., & Dargahi, T. (2018). Cyber Threat Intelligence. Cham: Springer.

Denkers, A.J.M., Peeters, M.P. & Huisman, W. (2013). Waarom organisaties de regels naleven: Over individuele motieven, de ethische bedrijfscultuur en de mores in de branche. Den Haag: Boom Lemma.

Faber, W. (2011). Financieel-economische criminaliteit? We kunnen niet zonder! Apeldoorn: Politieacademie.

Gorsira, M., Steg, L., Denkers, A., & Huisman, W. (2018). Corruption in organizations: Ethical climate and individual motives. Administrative Sciences, 8(4), 1-19.

Gunz, S. & Thorne, L. (2015). Introduction to the Special Issue on Tone at the Top. Journal of Business Ethics, 126(1), 1-2.

Hardy, C. & Levine, L. (2018). The Control Paradox. The EDP Audit, Control, and Security Newsletter, 58(1), 1-18.

Huisman, W. (2021). 'Corona, criminaliteit en strafrechtspleging'. Delikt en Delinkwent, 37(x).

IIA (2013). The three lines of defense in effective risk management and control. IIA. 1-10.

Key, S. (1999). Organizational Culture: Real or Imagined? Journal of Business Ethics, 20(3), 217-225.

Leukfeldt, E.R. (2014). Cybercrime and social ties: Phishing in Amsterdam. Trends in Organized Crime, 17(4), 231-249.

Meerts, C.A. (2018). The Semi-Autonomous World of Corporate Investigators: Modus vivendi, legality and control (Proefschrift). Erasmus Universiteit, Rotterdam.

Oates, B.J. (2006). Researching Information Systems and Computing. Londen: SAGEPublications. Oxford University Press. (2016). Oxford Dictionary. Oxford: Oxford University Press.

Payne, B.K. (2018). White-Collar Cybecrime: White-Collar Crime, Cybercrime or, Both?. Criminology, criminal justice, law & Society, 19(3). 16-32.

Rijksoverheid. (2021, 21 mei). Wetsvoorstel verbetert positie klokkenluiders. Rijksoverheid https://www.rijksoverheid.nl/actueel/nieuws/2021/05/21/klokkenenluiders.

Wagen, Van der, W., Oerlemans, J.J. & Weulen Kranenbarg, M. (2020). Basisboekcybercriminaliteit: Een criminologisch overzicht voor studie en praktijk. Den Haag: Boom criminologie.

Weijer, S. van de, Leukfeldt, E.R., Zee, S. van der. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. Policing: An International Journal.

Colofon

Projectteam PwC
Drs. Andreas Mikkers RA
Drs. Sebastiaan van Zijl
Reggie Hoost
Job Jebbink

Methodologie en validatie
Faculteit der Rechtsgeleerdheid, sectie Criminologie Vrije Universiteit Amsterdam
Prof. Dr. Wim Huisman
Dr. Clarissa Meerts

Extern onderzoeksbureau
Flycatcher Internet Research B.V.

In samenwerking met:

VU VRIJE UNIVERSITEIT AMSTERDAM

pwc

Bij PwC willen we een bijdrage leveren aan het vertrouwen in de maatschappij en het oplossen van belangrijke problemen. Wij zijn een netwerk van firma's in 158 landen met meer dan 250.000 mensen. Bij PwC in Nederland werken ruim 5.000 mensen met elkaar samen. Wij zien het als onze taak om kwaliteit te leveren op het gebied van assurance-, belasting- en adviesdiensten. Vertel ons wat voor u belangrijk is. Meer informatie over ons vindt u op www.pwc.nl.

© 2021 PricewaterhouseCoopers B.V. (KvK 34180289). Alle rechten voorbehouden. PwC verwijst naar de Nederlandse firma en kan soms naar het PwC-netwerk verwijzen. Elke aangesloten firma is een afzonderlijke juridische entiteit. Kijk op www.pwc.com/structure voor meer informatie.