Interne criminaliteit in de logistieke sector

G.B. Rovers
E. de Vries Robbé

Interne criminaliteit in de logistieke sector

G.B. Rovers
E. de Vries Robbé

B T V O

Bureau voor Toegepast **V**eiligheidsonderzoek

Voorwoord

Dankwoord

Dit onderzoeksrapport was niet tot stand gekomen zonder het advies en de bijdrage van een groot aantal personen en instellingen. In de eerste plaats bedanken wij de opdrachtgever van het onderzoek, het Wetenschappelijk Onderzoek- en Documentatiecentrum (afdeling Extern Wetenschappelijke Betrekkingen) van het ministerie van Justitie. Speciale dank zijn wij verschuldigd aan projectbegeleider Frans Beijaard voor zijn betrokkenheid, adviezen en het in ons gestelde vertrouwen.
Ook zijn wij bijzondere dank verschuldigd aan de leden van de begeleidingscommissie voor hun opbouwende kritieken en deskundig commentaar. Zij hebben een belangrijke waarde aan dit rapport toegevoegd. Hun namen zijn opgenomen in bijlage 4.
Daarnaast danken wij alle personen die hebben meegewerkt aan het onderzoek. Allen hebben zij waardevolle tijd vrijgemaakt om ons van dienst te kunnen zijn. Zonder het vertrouwen dat de respondenten bij de 139 bedrijven in ons hebben gesteld en de waardevolle en soms gevoelige informatie die zij met ons hebben gedeeld, had dit rapport niet geschreven kunnen worden. Wij hopen dat dit rapport voor deze bedrijven bijdraagt aan een veiliger ondernemingsklimaat.
De negentien experts die wij daarnaast hebben geraadpleegd, hebben eveneens een schat aan informatie aan het rapport toegevoegd. Waar het zicht van bedrijven beperkt was, konden zij aanvullen. De bijdrage van deze experts, waarvan de namen zijn opgenomen in bijlage 3, was voor dit rapport onmisbaar.
Ook bedanken wij de medewerkers van de infodesks van de verschillende politieregio's alsmede de medewerkers van de Centrale Justitiële Documentatie in Almelo. Zij hebben veel moeite moeten doen om ons van de gewenste informatie te voorzien. Het verzamelen van deze informatie was soms een hels karwei.
Ten slotte danken wij Karin van Wingerde en José Veldhuis. José Veldhuis heeft ons bijgestaan op die momenten dat wij het grote aantal interviews nauwelijks meer aan konden. Karin van Wingerde nam een belangrijk deel van het benaderen en het interviewen van de bedrijven op zich. Tevens danken we haar voor het samenstellen van de reader die wij aan de bedrijven beschikbaar hebben gesteld.
Al deze mensen hebben ertoe bijgedragen dat wij in korte tijd een goed beeld hebben kunnen krijgen van de logistieke sector in Nederland. Hun enthousiasme voor de sector hebben zij op ons overgedragen. Wij hopen dan ook met dit rapport een waardevolle bijdrage te kunnen leveren om het criminaliteitsprobleem binnen de logistieke dienstverlening aan te pakken.

Ben Rovers
Edo de Vries Robbé

's-Hertogenbosch, 18 april 2005

Inhoudsopgave

Samenvatting

Aanleiding en doelstelling van het onderzoek

In januari 2004 heeft het Nationaal Platform Criminaliteitsbeheersing (NPC) het 'Actieplan Veilig Ondernemen' gelanceerd, dat als belangrijkste doel kent: een reductie van criminaliteit gericht tegen het bedrijfsleven met minimaal 20% in 2008 (NPC, 2004a). Om dit te bereiken is een aantal projecten geformuleerd. Eén van deze projecten behelst de aanpak van interne criminaliteit. Een ander project behelst de aanpak van criminaliteit tegen de transport- en logistieke sector. Eén van de deelnemers aan het NPC, het ministerie van Justitie, heeft in dit kader het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) verzocht een onderzoek te laten uitvoeren naar interne criminaliteit in de logistieke sector. Dit rapport vormt hiervan de neerslag.
Het onderzoek beoogt inzicht te verschaffen in de aard en omvang van interne criminaliteit in de logistieke sector in Nederland. In het bijzonder de interne criminaliteit waarmee logistiek dienstverleners te maken hebben. Tevens wordt beoogd in kaart te brengen welke maatregelen deze logistiek dienstverleners treffen ter voorkoming van criminaliteit door medewerkers en op welke wijze zij reageren op concrete voorvallen. Hierbij wordt ook de rol van politie en justitie in ogenschouw genomen. De onderzoeksresultaten moeten het NPC ondersteunen bij het realiseren van preventieve en repressieve maatregelen tegen deze vorm van criminaliteit.

Onderzoeksvragen

Samengevat luiden de onderzoeksvragen:

- Wat is de aard en omvang van de interne criminaliteit bij logistiek dienstverleners in Nederland?
- Welke bedrijven worden slachtoffer en welke kenmerken hebben de daders van interne criminaliteit?
- Welke maatregelen treffen bedrijven in deze sector ter voorkoming van interne criminaliteit en op welke wijze reageren zij op concrete voorvallen?
- Hoe worden aangiften van interne criminaliteit door politie en justitie afgehandeld?

Definitie van interne criminaliteit

Onder interne criminaliteit verstaan wij opzettelijk normovertredend gedrag van werknemers (eventueel in samenwerking met anderen) dat is gericht tegen het bedrijf waar of waarvoor men werkzaamheden verricht (of verrichtte) en waarbij voor het bedrijf een schade optreedt of kan optreden die als problematisch wordt ervaren.

Opzet van het onderzoek

Gegevens over de aard en omvang van interne criminaliteit zijn niet in enige bestaande bron terug te vinden. Ook in politiële en justitiële registraties wordt interne criminaliteit niet als een aparte categorie behandeld. Om derhalve de eerste drie onderzoeksvragen te kunnen beantwoorden, hebben we bij 139 logistiek dienstverleners in Nederland een mondeling interview afgenomen (op basis van een deels gesloten en deels open vragenlijst). Het gaat om bedrijven voor wie *warehousing*, eventueel in combinatie met *Value Added Logistics* (VAL), een kernactiviteit vormt. *Warehousing* betekent dat de bedrijven de goederen niet alleen op- en overslaan, maar er ook 'iets' mee doen. Als deze bewerkingen waarde toevoegen aan de producten, zoals bij assemblage, reparatie en andere licht-industriële activiteiten, is sprake van VAL. Er bestaat geen administratief steekproefkader voor deze groep

bedrijven. Ze zijn derhalve geselecteerd via een aantal ledenlijsten van brancheorganisaties en andere logistieke koepels. Op deze lijsten komen 353 (unieke) bedrijven voor, waarvan 285 aan de steekproefcriteria voldeden. Bij 139 bedrijven (49%) hebben we een interview afgenomen, doorgaans met een persoon die binnen het bedrijf de meest deskundige is op het gebied van beveiliging. De bedrijven in het onderzoek vormen niet helemaal een representatieve doorsnede van de populatie (zoals vastgesteld op basis van de gehanteerde ledenlijsten): grote bedrijven en bedrijven gevestigd op Schiphol zijn oververtegenwoordigd in het onderzoek, kleine bedrijven en bedrijven gevestigd in Rotterdam zijn ondervertegenwoordigd. Deze factoren hangen deels samen: in Rotterdam bevinden zich naar verhouding meer kleine logistiek dienstverleners.
Naast de interviews in bedrijven zijn ook vijftien open interviews afgenomen met experts. Deze interviews dienden deels ter voorbereiding op de vragenlijst en deels ter validering van en aanvulling op de gegevens die zijn verkregen via de bedrijven. Hierbij gaat het onder meer om beleidsmedewerkers van brancheorganisaties in de logistiek, risicoconsultants, verzekeringsdeskundigen, opdrachtgevers van logistiek dienstverleners en private en politiële opsporingsdeskundigen.
Om de laatste onderzoeksvraag te kunnen beantwoorden, hebben we alle politieregio's in Nederland benaderd waar zich vestigingen bevinden van bedrijven uit ons onderzoek. We hebben hen de vraag voorgelegd of ze van de genoemde bedrijven aangiften hebben ontvangen in de periode 2002-2004 en zo ja, welke kenmerken deze aangiften hebben en of de misdrijven zijn opgehelderd. De verzamelde gegevens zijn vervolgens aangevuld met de gegevens die uit de bedrijven zijn verkregen. Met de verdachtengegevens van de opgehelderde aangiften is bij het Centraal Justitieel Documentatiesysteem in Almelo nagegaan of deze personen zijn vervolgd en zo ja, welke veroordeling eventueel is gevolgd.

Korte beschrijving van de onderzochte bedrijven

Bijna alle bedrijven zijn internationaal actief. Meer dan de helft van de bedrijven werkt met goederen die vanuit het oogpunt van diefstal kunnen worden beschouwd als goederen met een hoog risico. De omvang van de ondernemingen varieert: ruim een kwart heeft minder dan vijftig werknemers in Nederland, de rest van de bedrijven is middelgroot of groot (dat wil zeggen heeft vijftig tot tweehonderd werknemers of meer dan tweehonderd werknemers). Bijna tweederde van de bedrijven doet zelf niet aan transport of besteedt dit (grotendeels) uit. De bedrijven in het onderzoek zijn geografisch geconcentreerd in bepaalde gebieden in Nederland, zoals Schiphol, Rotterdam (haven en agglomeratie), Noord-Brabant (vooral Moerdijk, Tilburg en Eindhoven) en Limburg (vooral Venlo).

Belangrijkste onderzoeksbevindingen

Aard en omvang van gerapporteerde interne criminaliteit

Bedrijven zien interne criminaliteit als een minder groot probleem dan externe criminaliteit. Bijna de helft van de bedrijven (48%) noemt interne criminaliteit een probleem waarmee ze soms of vaker te maken hebben. Bijna één op de vijf bedrijven (18%) noemt interne criminaliteit een groot probleem. Van de bedrijven is 87% in de afgelopen drie jaar tenminste één keer slachtoffer geworden van enige vorm van interne criminaliteit. Gemiddeld noemen bedrijven elf interne incidenten in de afgelopen drie jaar. De helft van de getroffen bedrijven rapporteert minder dan vijf interne incidenten over de afgelopen drie jaar.
De meeste bedrijven rapporteren slachtofferschap van enige vorm van verduistering. Dit wordt door 61% van de bedrijven gerapporteerd. Verduistering is ook de vorm van interne criminaliteit waarvan bedrijven de meeste incidenten rapporteren. Hierbij gaat het in de meeste gevallen om tamelijk kleinschalige vormen van verduistering, zoals loodsmedewerkers die één product of één doos meenemen. Echter, ook verduisteringen van grote partijen (dure) goederen worden regelmatig gerapporteerd.
34% van de bedrijven rapporteert slachtofferschap van enige vorm van inbraak waarbij vermoedelijk of concreet sprake was van interne betrokkenheid. Het betreft hier niet alleen inbraken in loodsen en

kantoren, maar vooral inbraken in of diefstal van vrachtauto's (ladingdiefstal). Vaker dan bij voornoemde verduisteringen gaat het hierbij om grootschalige incidenten waarvan bedrijven veel schade ondervinden. Hoe grootschaliger de diefstal, des te groter ook de kans dat buitenstaanders erbij zijn betrokken.
29% van de bedrijven maakt melding van het feit dat ze slachtoffer zijn geworden van medewerkers die verwijtbaar onprofessioneel of nalatig gedrag hebben vertoond. Hierbij gaat het in de meeste gevallen om medewerkers die tegen de regels in bepaalde (veiligheids)procedures niet hebben gevolgd, waardoor een misdrijf kon plaatsvinden (vaak een inbraak of verduistering van een grote partij handelsgoederen).
17% van de bedrijven rapporteert dat ze in de afgelopen drie jaar te maken hebben gehad met verbaal of fysiek geweld onder collega's. Een vergelijkbaar aantal bedrijven rapporteert ervaringen met fraude. Bij de fraudegevallen is een duidelijk onderscheid te maken tussen kleine en grote fraude. De kleine fraude, het meest gemeld, betreft meestal gerommel met onkostendeclaraties, teveel uren schrijven en sjoemelen met vrachtbrieven. De grote fraude betreft meestal leidinggevenden of medewerkers met specialistische (financiële) functies die hun bevoegdheden en vrijheid gebruikt hebben om zichzelf te bevoordelen. Van alle gerapporteerde incidenten laten de fraudegevallen gemiddeld de hoogste schades zien.
11% van de bedrijven rapporteert dat men slachtoffer is geworden van medewerkers die ongeoorloofd bedrijfsmiddelen voor privé-doeleinden hebben gebruikt. Een vergelijkbaar aantal bedrijven rapporteert dat medewerkers gevoelige bedrijfsinformatie hebben doorgespeeld aan concurrenten. Bij de laatste categorie gaat het vaak om inmiddels ex-werknemers die met onenigheid zijn vertrokken uit het bedrijf (en zijn overgestapt naar de concurrent).
Daarnaast hebben we ook verschillende andere normovertredingen met de bedrijven besproken. Deze zijn door minder dan 10% van de bedrijven gerapporteerd. Hierbij gaat om zaken als sabotage van bedrijfsprocessen (9% van de bedrijven meldt slachtofferschap), opzettelijke vernieling (8%), (interne betrokkenheid bij) overvallen en corruptie (beide 5%), oplichting, illegale handel en medewerkers die bedrijfsmiddelen gebruiken voor commerciële activiteiten ten eigen bate (beide 3%).
Veel criminaliteit waarmee bedrijven te maken hebben is op enigerlei wijze transportgerelateerd. Dit zien bedrijven ook als het grootste criminaliteitsprobleem in hun sector. Hierbij kan het gaan om overvallen, inbraken in vrachtauto's en diefstallen van of uit vrachtauto's. Als het gaat om alle incidenten, dus niet alleen de interne incidenten, dan worden inbraken (inclusief vrachtauto- en ladingdiefstallen) door de meeste bedrijven gerapporteerd: 77% is hiervan in de afgelopen drie jaar tenminste één keer slachtoffer geworden. Van alle inbraakincidenten die bedrijven aan ons gemeld hebben, vermoeden ze in 14% van de gevallen interne betrokkenheid.

Dark number

De hiervoor gepresenteerde bevindingen zijn gebaseerd op de rapportage door bedrijven zelf. We weten echter dat hierbij allerlei onderrapportage-effecten optreden. Deze zorgen ervoor dat niet alle interne incidenten in de rapportage terecht komen. Interne incidenten als bijvoorbeeld fraude en illegale handel kunnen verborgen blijven in het bedrijf, omdat ze weinig of geen zichtbare sporen nalaten. Verduistering is een vorm van interne criminaliteit die als gebeurtenis vaak wel aan het licht komt, bijvoorbeeld in de vorm van vermissing van goederen, maar waarbij het voor bedrijven niet altijd mogelijk is om na te gaan wat er nu precies aan de hand is (verduistering is slechts één verklaring voor een vermissing). Ook hebben bedrijven niet altijd belang bij het labelen van een vermissing als verduistering, ze kunnen dan bijvoorbeeld aansprakelijk worden gesteld door de eigenaar of het is slecht voor hun imago. Soms zijn bedrijven zich gewoon ook weinig bewust van het feit dat vermiste goederen kunnen duiden op interne criminaliteit, ze houden er geen rekening mee. De gerapporteerde verduisteringen vormen daarom het topje van de ijsberg. Gebeurtenissen kunnen wel als normovertreding aan het licht komen, maar bedrijven zijn niet altijd bereid of in staat om interne betrokkenheid te signaleren. Dit probleem speelt vooral bij veel transportgerelateerde criminaliteit. Hierbij gaat het om overvallen, inbraken en grootschalige diefstallen van handelsgoederen. Het signaleren van interne betrokkenheid bij deze gevallen blijkt samen te hangen met veiligheidsbewustzijn en kennis: hoe hoger het veiligheidsbewustzijn in bedrijven en hoe meer kennis men heeft van feiten en omstandigheden rond deze incidenten, des te vaker zijn bedrijven in staat

interne betrokkenheid te vermoeden of aan te tonen. Overigens kunnen ook hier economische overwegingen een rol spelen om de interne betrokkenheid niet toe te geven (aansprakelijkheidsstelling door de verlader, et cetera). Om allerlei redenen hebben respondenten soms een beperkt zicht op wat er in het bedrijf omgaat. Ze werken er bijvoorbeeld pas kort of ze zien slechts wat er gebeurt in de vestiging waar ze zelf werken. Of hun zicht is beperkt tot bepaalde vormen van interne criminaliteit. Als ze wel een goed zicht hebben, zijn ze niet altijd bereid om hierover in alle gevallen te rapporteren aan de onderzoekers. Hierbij spelen bedrijfsmatige overwegingen een rol zoals hiervoor genoemd, maar soms hebben respondenten ook een persoonlijk belang om bijvoorbeeld een gunstiger beeld te schetsen van de situatie in het bedrijf.
Aanvullend onderzoek naar de interne betrokkenheid bij allerhande vormen van transportgerelateerde criminaliteit, het probleem waarvan de sector de meeste last zegt te ondervinden, bracht aan het licht dat bij deze vorm van criminaliteit, die bedrijven meestal als extern definiëren, in heel veel gevallen toch sprake is van interne betrokkenheid. Volgens alle door ons geraadpleegde ervaringsdeskundigen wordt zeker bij grootschalige diefstal van handelsgoederen (van/uit vrachtauto's en uit loodsen) in de meeste gevallen (sommige deskundigen zeggen: in alle gevallen) gebruik gemaakt van kennis van binnenuit. Dit beeld wijkt sterk af van het beeld dat bedrijven hierover hebben geschetst. We concluderen op grond van deze bevindingen, dat ook bij deze vorm van ('externe') criminaliteit in veel gevallen (toch) sprake is van interne betrokkenheid.

Kenmerken van bedrijven die slachtoffer worden van interne criminaliteit

De kenmerken van bedrijven die in het algemeen het sterkst zijn gerelateerd aan prevalentie en frequentie van interne criminaliteit zijn achtereenvolgens:

- De *omvang* van het bedrijf (hoe groter, des te meer criminaliteit);
- Problemen met *werving* van personeel (bij problemen meer criminaliteit);
- De aard van *bedrijfsactiviteiten* (hoe meer transportgerelateerd, des te meer criminaliteit);
- De aanwezigheid van hoog-risicovolle *goederen* (bij aanwezigheid meer criminaliteit).

Ook zaken als beveiligingsniveau en de aanwezigheid van extern personeel zijn gerelateerd aan het niveau van interne criminaliteit. Deze relaties verdwijnen echter als we rekening houden met de hiervoor genoemde factoren. De samenhang tussen beveiligingsniveau en het niveau van interne criminaliteit in een bedrijf is overigens een ingewikkelde, omdat veel bedrijven hun beveiliging opschalen naar aanleiding van incidenten die plaatsvinden. Dus in plaats van een negatief verband zien we hier een positief verband: beter beveiligde bedrijven rapporteren meer interne criminaliteit. Dit betekent uiteraard niet dat beveiligingsmaatregelen géén effect hebben op het terugdringen van interne criminaliteit. Het is alleen moeilijk vast te stellen in een onderzoek als het onderhavige.
Opvallend is verder dat de bedrijven in Rotterdam significant minder (interne) criminaliteit rapporteren dan bedrijven in andere regio's. Dit verschil wordt deels verklaard door het feit dat de door ons onderzochte bedrijven in deze regio vaak klein zijn en geen eigen transportfunctie hebben. Echter, ook als we hiermee rekening houden, blijken Rotterdamse bedrijven minder incidenten te rapporteren dan vergelijkbare bedrijven elders in het land. Onze onderzoeksgegevens bieden geen concrete aanknopingspunten om dit verschil te verklaren.
Ten slotte is het van belang hier op te merken dat sommige vormen van (interne) criminaliteit veel gevoeliger zijn voor verschillen in de hier genoemde bedrijfskenmerken dan andere. Het niveau van verduistering, vernieling of fraude varieert doorgaans sterker met de hier genoemde kenmerken dan bijvoorbeeld inbraak. Bij dit laatste misdrijf zijn de verschillen tussen bedrijven doorgaans veel geringer. Dat wil zeggen, alle bedrijven hebben hier in ongeveer gelijke mate last van.

Kenmerken van daders van interne criminaliteit

Bedrijven noemen zeer uiteenlopende kenmerken als het gaat om de achtergronden van personen die ooit concreet werden verdacht van enige vorm van interne criminaliteit. In de persoonlijke sfeer noemen ze vaak privé-problemen (met name geldproblemen, maar ook wel andere sociale problematiek zoals verslaving, echtscheiding en dergelijke), demografische kenmerken (vaak lager

opgeleiden, jonge mannen, soms allochtonen), persoonlijkheidskenmerken (een gebrekkig ontwikkeld normbesef, op te grote voet willen leven, roekeloos of kickgedrag), een crimineel verleden of personen die deel uitmaken van een criminele subcultuur of een crimineel netwerk. Ook als het gaat om de relatie die deze personen hebben tot het bedrijf worden zeer uiteenlopende kenmerken genoemd. Vaak genoemd zijn bijvoorbeeld tijdelijke krachten en personeel dat kort in dienst is, maar bijna even vaak is gemeld dat de betrokken werknemers juist al lang in dienst waren. In de meeste gevallen noemen bedrijven personeel op de werkvloer. Hierbij gaat het vaak om uitvoerend personeel, maar in een aantal gevallen ook om toezichthoudend of controlerend personeel. Ook specialistische of leidinggevende functies zijn genoemd. Ten slotte is ook onvrede van werknemers een aantal keren genoemd als kenmerk dat verband hield met de gepleegde feiten.
We moeten bij deze bevindingen opmerken dat de genoemde kenmerken uiteraard samenhangen met de vormen van criminaliteit die de respondenten in hun bedrijf waarnemen. Bij het doorspelen van gevoelige bedrijfsinformatie aan concurrenten zien de kenmerken van de daders er doorgaans anders uit dan bij diefstal uit de loods. Respondenten die slechts een enkele keer met verdachten van interne criminaliteit te maken hadden gehad, melden vaak dat de dader uit totaal onverwachte hoek kwam (harde werker, loyaal aan het bedrijf, al lang in dienst, nooit problemen, et cetera). Respondenten die juist heel veel ervaring hadden met interne verdachten, meldden ons vaak dat zij niet in staat waren om standaardkenmerken aan te wijzen, omdat de achtergronden van de personen daarvoor te verschillend waren. Als we deze twee antwoordcategorieën leggen naast het gegeven dat de overige respondenten de meest uiteenlopende achtergrondkenmerken noemen, zijn we geneigd te concluderen dat bij het plaatsvinden van interne criminaliteit, de persoonlijke en professionele achtergrond van de dader kennelijk van minder belang zijn dan de gelegenheidsstructuur. Hierbij mag overigens niet uit het oog worden verloren dat een klein deel van de werknemers, op grond van hun criminele verleden en hun criminele connecties, wel degelijk als een verhoogd risico moet worden beschouwd voor bedrijven. Het zou echter fout zijn te denken dat dit de enige risicogroep is.

Het treffen van preventieve maatregelen

Het is niet goed mogelijk om het preventiebeleid ten aanzien van interne criminaliteit goed af te bakenen van het preventiebeleid dat is gericht op externe criminaliteit. In veel bedrijven speelt dit onderscheid niet. Gemiddeld genomen blijken bedrijven in deze sector een scala aan preventiemaatregelen te nemen om (interne) criminaliteit tegen te gaan. Slechts een kleine groep van bedrijven is heel laag beveiligd, maar hierbij gaat het doorgaans om kleine bedrijven met weinig risicovolle goederen. In de grote groep van middelmatig beveiligde bedrijven wordt standaard een reeks van maatregelen genomen om (interne) criminaliteit tegen te gaan. Hierbij gaat het vooral om bouwkundige en technologische maatregelen, zoals toegangsbeveiliging met hekken, camera's, het gebruik van detectie- en alarminstallaties, et cetera. Een kleinere groep van (vooral grote) bedrijven onderscheidt zich door zeer uitgebreide veiligheidsprocedures. In deze groep zien we naast de hiervoor genoemde maatregelen vaak ook veel aandacht voor allerhande (controle)procedures, zoals controles op mensen en goederen door middel van visitatie, uitgebreide screening van toekomstig personeel en dergelijke. Er lijkt een volgorde te zitten in de preventiemaatregelen die minder en meer beveiligde bedrijven nemen: men begint doorgaans met bouwkundige en technopreventieve maatregelen, daarna volgt de nadruk op (controle van) allerlei bedrijfsprocedures, maar omdat de aandacht hiervoor vaak weer verslapt (en omdat deze procedures op gespannen voet kunnen staan met bedrijfseconomische uitgangspunten) zien we met name in de best beveiligde bedrijven weer een beweging naar het gebruik van mechanismen van informele sociale controle (die in kleine bedrijven min of meer vanzelf plaatsvinden). Hoe groter de onderneming, hoe risicovoller de goederen en hoe uitgebreider de bewerkingen die men op deze goederen pleegt, des te hoger ligt doorgaans het beveiligingsniveau.
De nadruk in het preventiebeleid ligt bij de meeste bedrijven op het voorkómen van diefstal van handelsgoederen. Dit zien bedrijven als het grootste criminaliteitsrisico. Een aantal bedrijven noemt ook het vitale belang van hun informatiesystemen. Diefstal van geld vormt voor de meeste bedrijven geen risico (behoudens de bedrijven die met remboursementen werken). Hoewel meer dan de helft van de bedrijven zegt dat fraudebeleid een integraal onderdeel vormt van de bedrijfsvoering, hebben we niet het idee gekregen dat fraude (in de zin van vervalsing/manipulatie van documenten en dergelijke) prominente aandacht heeft in de sector.

Bedrijven hebben wisselende opvattingen over welke maatregelen effectief zijn. Dit hangt vooral af van het stadium waarin ze zich qua beveiliging bevinden: bedrijven die net een hek hebben geplaatst rond hun bedrijfsterrein zijn doorgaans erg te spreken over de preventieve werking hiervan. Hetzelfde geldt voor bedrijven die net camera's hebben geplaatst. In de hoogbeveiligde bedrijven zijn ze vaker tevreden over visitatieprocedures, maar in sommige van deze bedrijven noemt men alweer de tekortkomingen hiervan en stelt men zich op het standpunt dat sociale-controlemechanismen aanvullend moeten worden gebruikt, omdat technopreventieve maatregelen en controleprocedures altijd kunnen worden omzeild.
Met uitzondering van een aantal grote, goed beveiligde ondernemingen, zien we dat veel bedrijven hun preventieve maatregelen vooral reactief nemen, dat wil zeggen in reactie op incidenten waarmee ze te maken hebben. Dit heeft vooral financiële achtergronden, want veel bedrijven noemen de financiën een obstakel bij het treffen van preventieve maatregelen. Ze zullen deze pas nemen als het niet anders kan. Naast economische afwegingen speelt hierbij de druk van externe partijen, zoals verzekeraars en opdrachtgevers, een rol. Andere obstakels die bedrijven ervaren bij het treffen van preventieve maatregelen liggen op het juridische en organisatorische vlak. Bij juridische obstakels gaat het vaak om beperkingen die de privacywetgeving oplegt aan bijvoorbeeld het toepassen van cameratoezicht of het uitvoeren van visitaties. Ook rapporteren bedrijven nogal eens personeelsverzet tegen allerhande toezicht- en controlemaatregelen. Dit speelt echter vooral in kleinere bedrijven.

Reactie van bedrijven op concrete voorvallen van interne criminaliteit

Hiervoor hebben we al geconstateerd dat met uitzondering van een aantal grote bedrijven, veel bedrijven op concrete incidenten reageren met aanpassingen in de beveiliging of in organisatieprocedures. Verder zien we dat de reacties op concrete voorvallen sterk afhangen van het soort voorval dat zich voordoet en de omstandigheden die hierbij aan de orde zijn. Zo voeren bedrijven bij verduistering vaker een intern onderzoek uit dan bijvoorbeeld bij inbraak (waarbij sprake is van interne betrokkenheid). Bij dergelijke 'interne' inbraken doen bedrijven weer veel vaker aangifte dan bij verduistering. Bij fraude is zelden sprake van aangifte. Het inschakelen van een recherchebureau doen bedrijven vaak pas als sprake is van een zekere schadeomvang. In het algemeen geldt echter dat hoe groter de schade van het betreffende incident, des te uitvoeriger de maatregelen die men treft.
De reacties ten aanzien van de daders van interne criminaliteit zijn homogener. In veruit de meeste gevallen (als het gaat om eigen medewerkers) wordt ontslag aangezegd of aangedrongen op 'vrijwillig' ontslag (onder bedreiging van het doen van aangifte). Bij lichtere normovertredingen, zoals nalatigheid, volgt vaak een waarschuwing of een aantekening in het personeelsdossier. De gang naar de strafrechter of de civiele rechter (om de schade te verhalen) wordt zelden gemaakt. Het zijn vooral enkele grote bedrijven die dit als standaardbeleid hebben. Heel veel bedrijven klagen juist over het feit dat deze trajecten voor hen doorgaans weinig opleveren en dat ze (te)veel tijd en geld kosten. Een aantal bedrijven is uitgesproken gefrustreerd over de ontslagprocedure bij de civiele rechter, omdat ze daar geconfronteerd werden met het feit dat hun ontslaggronden onvoldoende werden bevonden (door een gebrek aan bewijs of onrechtmatig verkregen bewijs). Hierdoor moesten ze de vermeende dief ook nog eens schadeloos stellen of weer in dienst nemen. De bewijskwestie weerhoudt veel bedrijven dan ook ervan om dit traject te bewandelen. Men kiest er in deze gevallen eerder voor om met de medewerker tot een onderling vergelijk te komen aangaande compensatie van de schade.
Wat betreft het doen van aangifte bij de politie, kunnen we constateren dat enkele, met name grote bedrijven, dit als standaardbeleid hebben, maar voor de meeste bedrijven geldt dat ze alleen aangifte doen als het moet (vanwege de verzekering) of als ze een concrete verdachte hebben waar ze vanaf willen. Als er geen interne of externe noodzaak is om aangifte te doen, geven bedrijven er in veruit de meeste gevallen de voorkeur aan om de zaak intern af te handelen.

Afhandeling van interne aangiften door politie en justitie

Als we kijken naar de wijze waarop aangiften van interne criminaliteit door politie en justitie worden afgehandeld, zien we in grote lijnen een bevestiging van het beeld dat bedrijven ons geschetst hebben: de door de politie opgehelderde interne zaken die wij hebben onderzocht, bestaan voor het overgrote deel uit aangiften waarbij bedrijven zelf de verdachten 'aanleverden'. Als deze informatie niet voor

handen was, bleek de kans op opheldering minimaal. Bovendien werd slechts in een minderheid van de gevallen waarin een aangifte werd opgehelderd, overgegaan tot vervolging van verdachten. In de meeste gevallen werd de zaak geseponeerd (52%). Heel vaak ging het hierbij zelfs om zaken met verdachten die al een strafblad hadden (in 67% van de gevallen). Als er al vervolgd werd bestond de zwaarste sanctie in 66% van de gevallen uit een geldboete of een taakstraf.
Veel bedrijven zullen hierin een bevestiging zien dat politie en justitie tekortschieten bij de aanpak van criminaliteit waardoor men getroffen wordt. Echter, ook bedrijven zelf nemen niet altijd hun verantwoordelijkheid als het gaat om de strafrechtelijke afhandeling van criminaliteit. Zo doen ze vaak geen aangifte of ze trekken zich in een later stadium terug uit het strafrechtelijke traject, omdat het hen in deze gevallen beter uitkomt om de zaak intern en/of civielrechtelijk af te handelen. Dit vermindert de mogelijkheden van politie en justitie om verdachten op te sporen en te vervolgen.

Tot besluit

Wij kunnen stellen dat de logistieke dienstverlening kwetsbaar is voor (serieuze vormen van) criminaliteit. Dit blijkt uit de aard en omvang van de incidenten die bedrijven aan ons gemeld hebben. Vaker dan door bedrijven wordt aangenomen is hierbij ook sprake van interne betrokkenheid. Ervaringen van terzake doende (opsporings)deskundigen wijzen duidelijk in deze richting. Zowel bedrijven zelf als ook brancheorganisaties en politiële en justitiële instanties kunnen nog het nodige verbeteren om deze problematiek tot een voor ieder aanvaardbaar niveau terug te brengen.

1 Achtergrond, probleemstelling en opzet van het onderzoek

Ruim de helft van alle bedrijven in Nederland wordt jaarlijks minimaal één keer slachtoffer van enige vorm van criminaliteit en bijna een kwart van de bedrijven is meervoudig slachtoffer, zo blijkt uit onderzoek van het NIPO (2002). Criminaliteit is voor het bedrijfsleven een alledaags probleem met alle gevolgen van dien. De directe en indirecte materiële schade bedraagt jaarlijks volgens het NIPO circa 1,3 miljard euro (2002). Daarbij komen nog de kosten voor het treffen van preventieve maatregelen. Er zijn echter ook immateriële gevolgen: het persoonlijk leed van medewerkers en eigenaren, de moeilijkheden die bedrijven kunnen ondervinden bij het verzekeren en financieren van hun bedrijf, het behouden of vinden van goed personeel, imagoschade, et cetera.
In 1992 is het Nationaal Platform Criminaliteitsbeheersing (NPC) opgericht. Dit is een publiek-privaat samenwerkingsverband tussen de landelijke overheid en het bedrijfsleven in Nederland, dat tot doel heeft de criminaliteit aan te pakken die gericht is tegen het bedrijfsleven. In januari 2004 heeft het NPC het 'Actieplan Veilig Ondernemen' gelanceerd, dat als belangrijkste doel kent: een reductie van de criminaliteit tegen het bedrijfsleven met minimaal 20% in 2008. Om dit te bereiken is een aantal projecten geformuleerd. Eén van deze projecten behelst de aanpak van interne criminaliteit. Een ander project behelst de aanpak van criminaliteit tegen de transport- en logistieke sector. Eén van de deelnemers aan het NPC, het ministerie van Justitie, heeft in dit kader het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) verzocht een onderzoek te laten uitvoeren naar interne criminaliteit in de logistieke sector. Dit rapport vormt hiervan de neerslag.

1.1 Doelstelling van het onderzoek

Het onderzoek beoogt inzicht te verschaffen in de aard en omvang van interne criminaliteit in de logistieke sector in Nederland. In het bijzonder betreft dit de interne criminaliteit waarmee logistiek dienstverleners te maken hebben. Tevens wordt beoogd in kaart te brengen welke maatregelen deze logistiek dienstverleners treffen ter voorkoming van criminaliteit door medewerkers en op welke wijze zij reageren op concrete voorvallen. Hierbij wordt ook de rol van politie en justitie in ogenschouw genomen. De onderzoeksresultaten moeten het NPC ondersteunen bij het realiseren van preventieve en repressieve maatregelen tegen deze vorm van criminaliteit in de logistieke sector.

1.2 Onderzoek naar interne criminaliteit in bedrijven

Empirische kennis over criminaliteit tegen het bedrijfsleven is schaars. Zeker wanneer dit wordt vergeleken met de hoeveelheid kennis die beschikbaar is over criminaliteit tegen natuurlijke personen. Kennis over interne criminaliteit is zo mogelijk nog schaarser.
Het aantal empirische studies naar interne criminaliteit in het bedrijfsleven is in Nederland op de vingers van één hand te tellen. Klassiek is de studie van Hoekema (1972) naar diefstal van havenarbeiders bij Rotterdamse stuwadoorsbedrijven. Het gaat hierbij om diefstal van goederen tijdens het laden en lossen van zeeschepen. Hoekema's onderzoek maakt duidelijk dat kleinschalige diefstal tijdens dit proces in die tijd heel vaak vóórkwam. Alleen voor deze vorm van diefstal maakte de Rotterdamse politie 'vele honderden processen-verbaal' per jaar op, volgens Hoekema het topje van de ijsberg. Het is moeilijk om de resultaten van deze studie naar het heden te extrapoleren. Enerzijds heeft dit te maken met het feit dat de genoemde werkzaamheden steeds meer geautomatiseerd zijn. Anderzijds is de in Hoekema's studie geschetste gelegenheidsstructuur er één die hedentendage bijzonder gedateerd aandoet: er werd toen gewerkt in kleine, autonome ploegen, waarbij nauwelijks of geen sprake was van toezicht of preventie in bredere zin. De werknemers hadden letterlijk 'alle gelegenheid' om spullen mee te nemen.
In de voornoemde NIPO-studie (Monitor Bedrijven en Instellingen 2002) is aan bedrijven gevraagd of ze in het afgelopen jaar slachtoffer zijn geworden van een bepaalde vorm van criminaliteit. Vervolgens is gevraagd of van het laatste delict de dader of vermoedelijke dader bekend is geworden en zo ja, wie

dit was (een klant of opdrachtgever, een personeelslid, een leverancier, et cetera)? De dader bleek in de meeste gevallen onbekend. Slechts in een zeer gering aantal gevallen wisten de betrokken respondenten te melden dat het om 'interne mensen' ging. Alleen bij gevallen van fraude lag dit percentage iets hoger (zo rond 13%).
De stichting TrendMeter[1] deed in 2000 in opdracht van werkgeversorganisatie VNO-NCW een onderzoek onder vierhonderd algemeen directeuren van middelgrote ondernemingen in Nederland (twintig tot vijfhonderd werknemers). Van hen zei 54% in de afgelopen drie jaar het slachtoffer geworden te zijn van enige vorm van interne criminaliteit. Hierbij ging het met name om diefstal van goederen (ruim éénderde), diefstal van geld (bijna 30%), fraude of verduistering (12%), diefstal van informatie (10%) en enige vorm van corruptie (2%). De onderzoekers merkten hierbij op dat de definities omtrent ontoelaatbaar gedrag in en tussen bedrijven nogal variëren: wat in het ene bedrijf toelaatbaar wordt geacht, is dat in het andere bedrijf niet, en wat op enig moment toelaatbaar is, hoeft dat later niet meer te zijn (en omgekeerd).
In 1998 verscheen een studie van Elzinga en Klerks (1998) naar de kenmerken en mogelijkheden voor een aanpak van interne criminaliteit. Deze studie is uitgevoerd in drie sectoren: het ziekenhuiswezen, de detailhandel en de distributiesector. Evenals de TrendMeter-onderzoekers wijzen zij erop dat er een grijs gebied bestaat van gedragingen van personeelsleden die niet als crimineel zijn te kenschetsen, maar eerder als 'niet integer'. De onderzoekers doen geen kwantitatieve uitspraken over prevalentie en frequentie van interne criminaliteit, omdat het verschijnsel zich lastig empirisch laat afbakenen. Bovendien stellen zij dat een groot deel van de incidenten onzichtbaar blijft. Zo is lang niet altijd duidelijk of sprake is van een vergrijp (opzet of vergissing?) en als dat wel het geval is, is vaak niet duidelijk of hiervoor een intern persoon verantwoordelijk is. Als dat wel duidelijk is, wordt het niet altijd gemeld aan de bedrijfsleiding of aan de politie. Bedrijven zelf staan ook niet te springen om openbaarmaking van deze gevallen. Er kan imagoschade optreden, de verzekerbaarheid van goederen kan gevaar lopen, et cetera (1998: 29). De bevindingen van Elzinga en Klerks maken duidelijk dat bij een meting van interne criminaliteit altijd rekening moet worden gehouden met een aanzienlijk *dark number*.
Enkele jaren geleden verscheen een studie van Van Dijk et al. (1999) naar de criminaliteitsrisico's van de logistieke keten in de haven van Rotterdam. Hierbij werd niet alleen gekeken naar bedrijven als slachtoffer, maar ook naar bedrijven als dader of als intermediair van criminaliteit. Er werd gekeken naar zowel externe als interne vormen van criminaliteit. De belangrijkste vormen van (interne én externe) criminaliteit die bedrijven -als slachtoffer- ervaren, bleken achtereenvolgens diefstal (van/uit containers, uit loodsen, van haventerreinen), inbraken (in loodsen), overvallen (in het wegtransport), heling, smokkel, fraude en corruptie (1999: 19). Deze incidenten komen doorgaans niet vaak voor, maar de schadebedragen per incident zijn gemiddeld genomen wel erg hoog. De studie van Van Dijk et al. bevat veel gedetailleerde (casus)beschrijvingen die tezamen een goed inzicht geven in de criminele gelegenheidsstructuur van de sector. De goederen- en documentenstroom in de logistiek worden daarbij het meest kwetsbaar geacht voor criminaliteit. Voor de geldstroom geldt dit in mindere mate. Ook in deze studie wijzen de onderzoekers erop dat het moeilijk is om een volledig overzicht te krijgen van voorvallen van interne criminaliteit. Zij brengen dit onder andere in verband met het feit dat bedrijven vaak onderdeel uitmaken van een soms lange en complexe logistieke keten. Aan het einde van deze keten (en soms ook eerder) blijken bijvoorbeeld goederen te ontbreken of zendingen niet in orde te zijn. Het is dan heel moeilijk om na te gaan waar in de logistieke keten iets fout is gegaan.
De meest uitgebreide Nederlandstalige studie in dit verband is die van Cools (1994). Zijn proefschrift over werknemerscriminaliteit bevat enerzijds een grondige conceptuele beschouwing over het fenomeen en doet anderzijds verslag van een tweetal empirische studies. Uit deze studie komt naar voren dat het vooral vermogensmisdrijven zijn waar bedrijven slachtoffer van worden. Deze komen vaak aan het licht doordat (ander) personeel melding ervan maakt. Ook Cools wijst op het feit dat het moeilijk is om een goed inzicht te krijgen in wat er op dit vlak allemaal omgaat in bedrijven. Sommige bedrijven monitoren hun bedrijfsprocessen beter dan andere bedrijven en komen daardoor ook meer op het spoor. Bovendien wijst hij erop dat als er al zicht bestaat op incidenten, de identiteit van de dader(s) of verdachte(n) meestal niet bekend is.

[1] Deze stichting is inmiddels opgeheven.

In het Engelse taalgebied, met name in de Verenigde Staten, is weliswaar meer empirisch onderzoek voorhanden naar interne criminaliteit in het bedrijfsleven, maar ook daar is het nog altijd een marginale 'tak van sport'. Interne criminaliteit geniet in de VS vooral academische aandacht van organisatie- en bedrijfskundige disciplines, waarbij de aandacht met name uitgaat naar thema's die verband houden met preventie en bestrijding (Traub, 1996; Jensen en Hodson, 1999). Overzichten van dit onderzoek zijn onder meer te vinden bij Green (1990), Murphy (1993), Giacalone en Greenberg (1997), Robinson en Greenberg (1998) en Mars (2001). De resultaten van deze en ook andere studies komen verderop in dit rapport aan de orde.

Samenvattend kunnen we stellen dat onze empirische kennis van interne criminaliteit in het bedrijfsleven schaars en fragmentarisch is. Wel is duidelijk dat het gaat om een verschijnsel dat zich om allerlei redenen moeilijk in kaart laat brengen. Dit heeft onder andere te maken met de wat vage contouren van het concept, waarbij graduele en vaak onduidelijke overgangen bestaan tussen toelaatbaar, ontoelaatbaar en crimineel gedrag. Daarnaast doen zich bij het vaststellen van dit verschijnsel in de praktijk tal van problemen van zeer uiteenlopende aard voor, die er gezamenlijk voor zorgen dat het fenomeen voor een deel onzichtbaar blijft.

1.3 Probleemstelling en onderzoeksvragen

Voor deze studie is de volgende probleemstelling geformuleerd:

> *Wat is de aard en omvang van de interne criminaliteit bij logistiek dienstverleners in Nederland? Welke maatregelen treffen bedrijven in deze sector ter voorkoming van interne criminaliteit en op welke wijze reageren zij op concrete voorvallen? Hoe gaan politie en justitie om met aangiften van interne criminaliteit?*

Deze probleemstelling omvat de volgende onderzoeksvragen:

Aard en omvang van interne criminaliteit in de logistieke sector

1 Wat is de aard en omvang van de interne criminaliteit waarmee logistiek dienstverleners in de afgelopen drie jaar zijn geconfronteerd?
2 Wat zijn de kenmerken van bedrijven die in meer of mindere mate met verschillende vormen van interne criminaliteit worden geconfronteerd?
3 Op welke wijze zijn de genoemde voorvallen van interne criminaliteit aan het licht gekomen en in hoeverre bestaan er binnen de bedrijven belemmeringen om een goed zicht op dit verschijnsel te hebben?
4 Welke relevante kenmerken hebben de bekende daders van de verschillende vormen van interne criminaliteit?

Preventieve maatregelen door bedrijven

5 Welke preventieve maatregelen hebben bedrijven getroffen om zich te beschermen tegen verschillende vormen van interne criminaliteit?
6 In hoeverre leiden veronderstelde of geconstateerde voorvallen van interne criminaliteit tot aanpassingen in het preventiebeleid? Welke obstakels doen zich hierbij mogelijk voor?

Reactie van bedrijven op concrete voorvallen

7 Welke (interne en externe) acties ondernemen bedrijven wanneer zij kennis nemen van vermeende of geconstateerde voorvallen van interne criminaliteit? In hoeverre bewandelen zij hierbij strafrechtelijke en/of civielrechtelijke wegen?

Afhandeling van aangiften

8 In hoeverre zijn bedrijven op de hoogte van de wijze waarop politie en justitie hun (eventuele) aangiften van interne criminaliteit hebben afgehandeld en wat is de daadwerkelijke *follow up* in deze gevallen geweest?

1.4 Enkele definities

In de probleemstelling worden enkele termen gebezigd die nadere toelichting behoeven. Hieronder worden de termen 'interne criminaliteit' en 'logistiek dienstverleners' nader omschreven.

1.4.1 Interne criminaliteit

In deze studie gaat onze aandacht uit naar normovertredend gedrag van werknemers in de logistieke sector. In de literatuur komen we uiteenlopende termen tegen die in enigerlei mate verwijzen naar de verzamelde empirische verschijnselen waarin wij in dit verband geïnteresseerd zijn. In de schaarse Nederlandstalige literatuur zijn de termen 'werknemerscriminaliteit' en 'interne criminaliteit' min of meer ingeburgerd. In de Engelstalige literatuur zijn het zulke diverse termen als *white collar crime*, *workplace deviance*, *antisocial behavior in organizations*, *employee vice*, *organizational misbehavior*, *non-compliant behavior*, *occupational crime, honesty in the workplace,* et cetera (Green, 1990; Murphy, 1993; Cools, 1994; Robinson en Greenberg, 1998). We kiezen ervoor in deze studie de aanduiding *interne criminaliteit* te hanteren, omdat deze vlag de lading het beste dekt en de term communicatief goed werkt.

Onze definitie van interne criminaliteit luidt als volgt:

- *Opzettelijk normovertredend gedrag van werknemers (eventueel in samenwerking met anderen);*
- *Dat is gericht tegen het bedrijf waar of waarvoor men werkzaamheden verricht (of verrichtte);*
- *En waarbij voor het bedrijf een schade optreedt of kan optreden die als problematisch wordt ervaren.*

Toelichting:
In onze definitie leggen we de term 'werknemer' breed uit. Het bedrijf dat slachtoffer wordt, geldt hierbij als focaal punt. Dit bedrijf heeft te maken met personen die hun beroep uitoefenen. Dit kunnen personen zijn die een vast of tijdelijk dienstverband hebben bij het bedrijf, maar ook uitzendkrachten, stagiaires, bezoekers, leveranciers, en allerhande werknemers die in dienst zijn van onderaannemers, zoals schoonmakers, ICT-deskundigen, onderhoudsmonteurs, et cetera. Het gemeenschappelijke is dat al deze personen vanuit hun hoedanigheid als werknemer (bij enig bedrijf) in contact staan met het bedrijf waarin wij geïnteresseerd zijn. Indien werknemers vanuit hun beroepsuitoefening toegang hebben tot een bedrijf (in welke vorm ook), gelden deze personen voor dit bedrijf als 'internen'. Kortom, niet het dienstverband is maatgevend om tot de internen te worden gerekend, maar de toegang tot het bedrijf. We kiezen daarom ook ervoor om onszelf niet te beperken tot normovertredend gedrag van *huidige werknemers* (zie Green, 1990). Als het gaat om toegang hebben tot het bedrijf (dus ook toegang tot informatie over het bedrijf), moeten ex-werknemers als een relevante categorie worden beschouwd. In sommige definities worden ook de organisaties zelf of de werkgevers als individuen, beschouwd als mogelijke regelovertreders (Green, 1990; Robinson en Greenberg, 1998). Deze categorieën laten we hier buiten beschouwing, omdat we daarmee op het vlak van de organisatiecriminaliteit komen en dat verschijnsel valt buiten het bestek van deze studie. Managers zijn uiteraard ook werknemers in een bedrijf en worden als zodanig tot de internen gerekend.
Uit de definitie volgt dat het gaat om gedrag dat als een normovertreding kan worden beschouwd. De voor de hand liggende vraag luidt dan: welke normen of wiens normen? Hier kunnen we een onderscheid maken tussen normovertredingen die strafbaar zijn gesteld bij wet (criminaliteit) en overige normovertredingen in bedrijven. Verduistering van goederen van de werkgever is een voorbeeld van het eerste, smokkelen met het in- en uitklokken op het werk is een voorbeeld van het

tweede. We kunnen de overige normovertredingen opdelen in (bedrijfs)normen die voor een specifiek bedrijf gelden (het personeel draagt in dit bedrijf alleen op vrijdag vrijetijdskleding) en normen die algemeen gelden (op tijd op het werk komen, niet onterecht ziek melden, het productieproces niet saboteren en dergelijke). In deze studie zullen we ons richten op criminaliteit en overtredingen van sociale- en bedrijfsnormen die algemeen gelden. Overtredingen van bedrijfsspecifieke normen blijven hier buiten beschouwing.
In sommige studies (zie hiervoor het overzicht in Robinson en Greenberg, 1998) is naar voren gebracht dat veel deviantie van werknemers eigenlijk normconform gedrag is als wordt gekeken naar de microsociale context waarin dit gedrag plaatsvindt. Gedrag dus dat voldoet aan de normen van een subcultuur. Het mag duidelijk zijn dat dit gedrag, indien het algemene sociale- of bedrijfsnormen overtreedt, hier wel degelijk onderwerp van studie is.
Een belangrijke kwaliteit die door veel onderzoekers wordt toegevoegd aan de normovertreding, is dat het moet gaan om *opzettelijk* gedrag (Robinson en Greenberg, 1998). Met andere woorden, een normovertreding die per ongeluk optreedt, 'telt niet mee'. Sommige auteurs voegen hier ook vrijwilligheid aan toe, maar dit begrip geeft veel conceptualiserings- en operationeliseringsproblemen. Wanneer is immers sprake van vrije wil? Als iemand de geldende normen in de subcultuur volgt? Als iemand onder de invloed van alcohol is? Wij volgen hier het gebruik om van interne criminaliteit te spreken indien sprake is van opzettelijk gedrag. Dit is ook in lijn met het belang van het begrip 'opzet' in het strafrecht. We zullen in de zijlijn van het onderzoek echter ook enige aandacht besteden aan het verschijnsel 'verwijtbare nalatigheid'. Dit betreft gedrag waarbij geen sprake is van opzet, maar wel van (grove) schuld (volgens de betreffende bedrijven).
Murphy (1990: 8) wijst erop dat bedrijven vaak een soort ondergrens hanteren om te bepalen welke normovertredingen ze nog acceptabel vinden en welke niet. Zo wordt verduistering van kleine items heel vaak niet beschouwd als onacceptabel (bijvoorbeeld het mee naar huis nemen van potloden en pennen van het werk). Hetzelfde geldt voor het voeren van korte privé-telefoongesprekken, incidenteel te laat komen, et cetera. Het trekken van deze grens heeft voor bedrijven ook te maken met de handhaafbaarheid van de gestelde regels: een *zero tolerance* beleid aangaande bijvoorbeeld triviale diefstallen (potloden/pennen) is niet of nauwelijks te handhaven. Wij kiezen ervoor deze 'grensproblematiek' (wat is toelaatbaar en wat niet meer?) te omzeilen door ons te richten op normovertredingen die, afzonderlijk of in hun totaliteit, een schade opleveren of kunnen opleveren die het bedrijf zelf als problematisch ervaart. Dit is uiteraard een subjectief criterium, waarmee bedrijven verschillend zullen omgaan, maar een voordeel van deze afbakening is dat we met bedrijven vooral kunnen spreken over zaken waarvan zij last ondervinden. Gelet op de beleidsachtergrond van dit onderzoek, lijkt ons dit een goed te rechtvaardigen keus. Uiteraard gaan we hiermee voorbij aan allerlei vormen van interne criminaliteit of interne normovertredingen die zich op de rand van het toelaatbare en ontoelaatbare afspelen.
Diverse auteurs hebben erop gewezen dat normovertredingen ook voordelig kunnen zijn voor een bedrijf. Bijvoorbeeld voor een bepaalde groep werknemers of zelfs voor het bedrijf als geheel (als de werknemer handelt in opdracht van de leiding) (Robinson en Greenberg, 1998). Een bedrijf kan bijvoorbeeld illegaal vervuilde grond of afval storten. Aangezien we ons hier beperken tot normoverschrijdend gedrag van werknemers gericht *tegen* bedrijven, is deze variant hier niet aan de orde.
Werknemers kunnen individueel een norm overtreden, maar uiteraard ook in samenwerking met anderen. Die anderen kunnen zowel internen als externen zijn. We spreken van interne criminaliteit als de betreffende normovertreding mogelijk is gemaakt door de beroepsuitoefening van tenminste één interne werknemer. Als het om een groep gaat is de betrokkenheid van tenminste één interne werknemer vereist.
In de literatuur wordt een scala van mogelijke doelwitten van interne criminaliteit genoemd, zoals het bedrijf zelf, de overheid, collega's, klanten, leveranciers, het algemene publiek, et cetera (Green, 1990; Robinson en Greenberg, 1998). Een algemeen onderscheid kan worden gemaakt tussen individuele doelwitten (stelen van/geweld tegen collega's, klanten of leveranciers) en organisatiedoelwitten. Een veel gebruikte verfijning van organisatiedoelwitten is voorgesteld door Hollinger en Clark (1982); zij onderscheiden *property deviance* (diefstal, beschadiging of misbruik van bedrijfsmiddelen) en *production deviance* (gedrag dat formele normen overschrijdt omtrent minimale kwaliteit en kwantiteit van te verrichten werk, zoals te laat komen, langzaam werken, onterecht ziekmelden, et

cetera). Het onderscheid tussen deze vormen van deviantie is soms gradueel: denk bijvoorbeeld aan een personeelslid die tijdens werkuren privé-ritten maakt met de auto van de baas en een personeelslid die hetzelfde doet, maar nu buiten werktijd. In deze studie beperken we ons in hoofdzaak tot normovertredingen die het bedrijf als doelwit hebben en zullen we beide door Hollinger en Clark (1982) genoemde categorieën in beschouwing nemen. Uitgesloten zijn derhalve normovertredingen gericht tegen collega's, klanten, leveranciers, et cetera.[2]
Het is niet uitgesloten dat normovertredingen gericht tegen deze groepen (indirect) ook het bedrijf kunnen schaden. Een verkoper of vertegenwoordiger die steelt van klanten, kan daarmee immers ook het bedrijf schade aandoen. Het criterium hier is echter niet wie uiteindelijk slachtoffer wordt van het gedrag, maar tegen wie de normovertreding is gericht. Zo zal een rancuneuze vertegenwoordiger (die niet de gevraagde loonsverhoging heeft gekregen) zijn werkgever kunnen schaden door onvriendelijk te zijn tegen klanten en dergelijke. In dit geval zou je kunnen stellen dat het bedrijf het doelwit vormt van de normovertreding (een vorm van *production deviance*) en de betreurenswaardige klanten niet meer zijn dan een middel tot dat doel.

Samenvattend kunnen we aangeven dat we een ruime definitie hanteren om aldus zoveel mogelijk problemen waarmee bedrijven te maken hebben, in kaart te kunnen brengen. Om deze reden zullen we tijdens het onderzoek ook soepel omgaan met grensgevallen, want het moge duidelijk zijn dat het niet moeilijk is om deze aan te treffen.

1.4.2 Logistiek dienstverleners

In de logistieke sector kunnen we enerzijds bedrijven aantreffen die eigenaar zijn van de goederen en/of diensten. Hierbij gaat het doorgaans om (onderdelen van) bedrijven die niet primair op logistieke dienstverlening zijn georiënteerd, maar voor wie logistieke activiteiten een bestanddeel vormen van bredere bedrijfsactiviteiten. Een voorbeeld is een winkelketen die zijn eigen transport, distributie, opslag en dergelijke regelt. Anderzijds vinden we in deze sector bedrijven die geen eigenaar zijn van de goederen of diensten. Deze bedrijven zijn primair georiënteerd op logistieke dienstverlening. Het onderzoek zal zich tot deze laatste categorie beperken, de zogenaamde 'logistiek dienstverleners'. Logistiek dienstverleners kunnen tal van diensten aanbieden, variërend van transport en distributie tot en met uitgebreide logistieke services, zoals facturering, douaneafhandeling en dergelijke.[3] Dit onderzoek beperkt zich tot bedrijven voor wie enige vorm van *warehousing* (eventueel in combinatie met *value added logistics*, VAL) een *kernactiviteit* vormt. *Warehousing* behelst primair op- en overslag van goederen waarop enige vorm van bewerking plaatsvindt. Het onderscheid tussen *warehousing* en op- en overslag is, dat in het laatste geval alleen sprake is van logistieke activiteiten, terwijl in het eerste geval logistieke activiteiten worden gecombineerd met (doorgaans lichte) industriële activiteiten. Het gaat hierbij meestal om eenvoudige bewerkingen op de goederen, zoals (her)verpakken van goederen, labelen/stickeren en dergelijke. Indien deze activiteiten waarde toevoegen aan de producten, zoals het geval is bij assemblage, kwaliteitscontrole, reparatie en dergelijke, is sprake van VAL.

1.5 Opzet van het onderzoek

Bestaande bronnen bieden geen bruikbare aanknopingspunten voor onderzoek naar interne criminaliteit. Het verschijnsel wordt, voor zover wij weten, in geen enkele politiële of justitiële registratie als een aparte categorie behandeld. Ook kennen wij geen andere bronnen die dit verschijnsel (in al zijn verschijningsvormen) in kaart brengen. De kern van het onderzoek bestaat daarom uit een mondelinge bevraging van circa 140 logistiek dienstverleners in Nederland. Dit onderzoek verschaft de antwoorden op bijna alle onderzoeksvragen die hiervoor zijn genoemd. Er is aanvullend onderzoek

[2] We maken hierop één uitzondering door wel het verschijnsel 'verbaal of fysiek geweld tegen collega's' te onderzoeken.
[3] Een handzaam overzicht van logistieke begrippen is te vinden op de website van Nederland Distributieland (NDL), in de kennisbank: www.ndl.nl.

gedaan bij politie en justitie om te zien hoe aangiften van interne criminaliteit (van deze bedrijven) strafrechtelijk zijn afgehandeld. Daarnaast zijn verschillende sleutelfiguren in het veld geraadpleegd. Deze raadpleging vond enerzijds plaats ter voorbereiding op het hoofdonderzoek (de bevraging van logistiek dienstverleners). Anderzijds is een aantal deskundigen gevraagd om de bevindingen uit het hoofdonderzoek aan te vullen en/of toe te lichten. In de paragrafen 1.5.1 en 1.5.2 wordt de opzet van het hoofdonderzoek besproken, in paragraaf 1.5.3 worden het politie-/justitieonderzoek en de deskundigenraadpleging nader toegelicht.

1.5.1 Selectie van bedrijven

Het onderhavige onderzoek richt zich op logistiek dienstverleners die in Nederland één of meer vestigingen hebben en voor wie *warehousing* (eventueel in combinatie met VAL) een kernactiviteit is. Van deze populatie van bedrijven is geen steekproefkader beschikbaar. Het register van de Kamer van Koophandel (KvK) biedt onvoldoende mogelijkheden om deze bedrijven te selecteren. De gehanteerde aanduidingen van bedrijfsactiviteiten zijn hiervoor ontoereikend.[4] Bijkomend probleem is dat de markt voor transport en logistieke dienstverlening sterk in ontwikkeling is. Veel bedrijven in de sector proberen hun activiteiten uit te breiden door ook activiteiten met een hogere toegevoegde waarde te ontwikkelen. Daar deze toegevoegde waarde voor veel bedrijven een groot deel van de omzet vormt, is dit voor veel bedrijven een kernactiviteit geworden. Ook het wegvallen van de Europese binnengrenzen heeft bijgedragen tot een grote dynamiek in de sector. Door de sterke concurrentie en kleine marges gaan regelmatig bedrijven failliet, ontstaan er nieuwe of worden bedrijven overgenomen. Navraag in de sector heeft ons bovendien geleerd dat het onderscheid tussen opslag, *warehousing*, VAL en VAS (*value added services*) door veel bedrijven nauwelijks wordt gemaakt, terwijl wij slechts geïnteresseerd zijn in bedrijven voor wie *warehousing* (eventueel in combinatie met VAL) een kernactiviteit is. Ook is niet altijd goed vast te stellen of het voor het bedrijf een kernactiviteit betreft: veel bedrijven beschikken over verschillende dochtermaatschappijen en/of verschillende vestigingen waar verschillende activiteiten plaatsvinden. Voor het in kaart brengen van de populatie van bedrijven die aan *warehousing* en VAL doen, hebben wij er daarom voor gekozen de ledenlijsten van diverse branche- en belangenorganisaties te gebruiken. Om de onderzoeksvragen goed te kunnen beantwoorden is de gewenste (netto) steekproefomvang vastgesteld op circa 140 bedrijven. De bedrijven in de 'populatie' zijn op basis van enkele relevante kenmerken in te delen. Dit zijn kenmerken die correleren met het onderzochte verschijnsel (interne criminaliteit). Elzinga en Klerks (1998) noemen in hun onderzoek de volgende relevante factoren voor interne criminaliteit: daderkenmerken en motieven, aantrekkelijke en bereikbare doelwitten, gelegenheidskenmerken en organisatiecultuur. In de Monitor Bedrijven en instellingen (NIPO, 2002) zijn correlaties gevonden tussen ondervonden criminaliteit enerzijds en bedrijfsomvang (in personele zin) en regionale ligging anderzijds: grote bedrijven in de randstad lopen een groter risico (het gaat hierbij om zowel interne als externe criminaliteit). Cohen en Felson (1979) onderscheiden in hun *routine activity theory* drie elementen welke noodzakelijk zijn om een delict plaats te laten vinden: aantrekkelijkheid doelwitten, afwezigheid van toezicht (gelegenheid) en de aanwezigheid van gemotiveerde daders. Ten aanzien van de aantrekkelijkheid van doelwitten merken Elzinga en Klerks (1998) op dat deze bij voorkeur een zekere waarde vertegenwoordigen, gemakkelijk beweegbaar en verplaatsbaar zijn, niet te omvangrijk zijn en bovendien (redelijk) toegankelijk. *De hypothese is hier dat bedrijven met meer aantrekkelijke goederen een grotere kans lopen om slachtoffer te worden van interne criminaliteit.* Afwezigheid van toezicht (of breder geformuleerd: de gelegenheid), wordt door tal van zaken beïnvloed (zie Elzinga en Klerks, 2002). Wij denken dat omvang van de onderneming (in aantal personeelsleden) een goede indicator is voor deze factor. Een indicator waarvan bovendien is gebleken dat hij correleert met de gerapporteerde (interne) criminaliteit door bedrijven. *De hypothese is hier dat grote ondernemingen meer gelegenheid bieden voor het plegen van interne criminaliteit, waardoor deze vaker slachtoffer zullen worden.* Ten slotte zal ook de aanwezigheid van gemotiveerde daders variëren. Het is moeilijk hiervoor een passende operationalisering te vinden. Wij gebruiken hiervoor als indicator de regionale

[4] Het gaat om de zogenaamde 'BIK-codes' (Bedrijfsindeling Kamer van Koophandel). Deze codes zijn afgeleid van de door het Centraal Bureau voor de Statistiek (CBS) gehanteerde SBI-codes (Standaard Bedrijfsindeling) en vormen daarop zelfs een verfijning.

en stedelijke ligging van bedrijven, ervan uitgaande dat in deze gebieden naar verhouding meer gemotiveerde daders wonen. *De hypothese is hier dat bedrijven in stedelijke gebieden in de randstad vaker slachtoffer zullen worden van interne criminaliteit dan bedrijven die gelegen zijn buiten de (rand)stad.* Dit levert drie relevante kenmerken op: 1) aantrekkelijkheid van doelwitten, 2) omvang van de onderneming en 3) regionale/stedelijke ligging.
Wij hebben ervoor gekozen om in elk bedrijf één respondent te bevragen, bij voorkeur de meest deskundige op het gebied van beveiliging. Bij kleine bedrijven is dit meestal de eigenaar/directeur of zijn/haar plaatsvervanger, bij middelgrote bedrijven een lijnfunctionaris die vaak ook belast is met integriteits- of beveiligingsvraagstukken. Bij grote bedrijven is vaak een functionaris speciaal belast met beveiliging. Elke keus van respondenten binnen een onderneming (bijvoorbeeld hoger geplaatst versus lager geplaatst personeel, staf- versus lijnfunctionarissen, et cetera) impliceert dat we bepaalde verschijnselen binnen de organisatie beter in beeld zullen krijgen dan andere (Van den Heuvel, 1997). Onze keus van respondenten heeft (zoals elke keuze) voor- en nadelen. Zo moet niet worden uitgesloten dat de hier genoemde functionarissen niet altijd op de hoogte zijn van wat er op de werkvloer van het bedrijf allemaal gebeurt. Ook is het mogelijk dat ze niet zo zijn geneigd om te praten over vormen van interne criminaliteit die zich in hun directe omgeving voordoen (bijvoorbeeld op hun eigen afdeling, bij de directie), laat staan dat ze willen praten over eventueel door henzelf gepleegde normovertredingen. Dit probleem doet zich echter ook voor bij andere soorten respondenten, zoals personen die op de werkvloer werken. Het nadeel van deze laatste groep is weer dat deze werknemers doorgaans het overzicht missen, waardoor veel werknemers per bedrijf moeten worden ondervraagd. Waar het gaat om het op bedrijfsniveau in kaart brengen van incidenten, preventiebeleid en dergelijke, lijkt deze laatste groep ons minder geschikt als respondenten voor het onderhavige onderzoek.
De bedrijven zijn telefonisch benaderd met de vraag welke functionaris in het bedrijf het meest belast is met *security*/beveiligingsaangelegenheden. Aan deze persoon is vervolgens een brief gestuurd waarin het onderzoek werd aangekondigd. Deze brief ging vergezeld van een aanbevelingsbrief die was ondertekend door directeuren van diverse brancheorganisaties in de logistiek (Transport en Logistiek Nederland [TLN], Nederland Distributieland [NDL], Koninklijk Nederlands Vervoer [KNV], EVO en Fenex). Enige tijd na het verzenden van de aankondiging zijn de respondenten telefonisch benaderd met de vraag of ze wilden meewerken aan een interview. Hierbij zijn enkele middelen ingezet om de respons te verhogen. Naast de voornoemde aanbevelingsbrief ging het hierbij om mededelingen betreffende waarborgen van vertrouwelijkheid bij deelname aan het onderzoek en de toezegging dat alle deelnemers het rapport zullen ontvangen alsmede een speciaal voor hen samengestelde reader met teksten over preventie van interne criminaliteit.

1.5.2 Opzet van de vragenlijst

De interviews bij bedrijven zijn mondeling afgenomen met behulp van een gestructureerde vragenlijst. Deze vragenlijst met aanhangsel, als bijlage 1 en 2 opgenomen bij dit rapport, bevat deels gesloten en deels open vragen (vaak gecombineerd). De keus voor gesloten vragen vloeit voort uit de behoefte de ervaringen van de betrokken bedrijven gemakkelijk te kunnen ordenen en kwantificeren. De open (gedeelten van de) vragen stellen ons in staat antwoorden/gegevens te verwerken die van tevoren niet kunnen worden voorzien. Daarnaast stellen deze vragen ons in de gelegenheid om meer diepgaand en in meer detail kennis te nemen van ervaringen van bedrijven.

De vragenlijst bevat zeven blokken:

1 Gegevens omtrent de afname van het interview;
2 Algemene bedrijfsgegevens en gegevens betreffende de functie van de respondent;
3 Gegevens over risico's, preventiebeleid en monitoring van bedrijfsprocessen;
4 Gegevens over (interne) normovertredingen en de reactie van het bedrijf daarop, alsmede gegevens over daderkenmerken;
5 Gegevens over de strafrechtelijke afhandeling van eventuele aangiften;
6 Slotopmerkingen van de respondent;
7 Observaties van de interviewer.

Ten aanzien van enkele onderdelen van deze vragenlijst is een nadere toelichting op zijn plaats.
De algemene vragen in blok 2 zijn enerzijds bedoeld om inzicht te krijgen in een aantal achtergrondkenmerken, zoals de omvang van het bedrijf, de geografische ligging van de *warehouses*, de schaal waarop de onderneming opereert, de productengroepen die men in de *warehouses* bewerkt, het type bewerkingen dat men verricht, de personele situatie, verzekeringskwesties, et cetera. Anderzijds zijn de vragen in dit blok bedoeld om in kaart te brengen in welke mate en op welke wijze *security*/beveiliging in een bedrijf onderdeel uitmaakt van de bedrijfsvoering.
De vragen in blok 3 zijn in eerste instantie bedoeld om de schaderisico's in kaart te brengen die bedrijven signaleren op het vlak van interne criminaliteit. Wat zijn de belangrijkste doelwitten, de meest kwetsbare bedrijfsprocessen, et cetera? Daarnaast is in dit blok een aantal vragen opgenomen over preventieve maatregelen. We hebben hierbij ervoor gekozen om zelf 26 preventieve maatregelen van zeer uiteenlopende aard voor te leggen aan de respondenten en te vragen of deze maatregelen ook worden getroffen in het betreffende bedrijf. Omdat hiermee onmogelijk een compleet beeld kan worden geschetst, is vervolgens gevraagd of er nog andere preventieve maatregelen worden getroffen. De respondenten is tevens gevraagd een oordeel te geven over de bijzondere (in)effectiviteit van bepaalde preventieve maatregelen (op grond van eerdere ervaringen). Ook obstakels bij het treffen van preventiemaatregelen, zoals te hoge kosten, juridische beperkingen en dergelijke, komen hier aan de orde. Ten slotte is in dit blok een aantal vragen voorgelegd over maatregelen en activiteiten die zicht geven op wat er in een bedrijf allemaal omgaat. Het idee hierachter is dat hoe meer bedrijven hun bedrijfsprocessen monitoren, des te beter ze in staat zullen zijn om vormen van interne criminaliteit op het spoor te komen. Omgekeerd kunnen deze monitoringsmaatregelen ook preventief werken, doordat werknemers weten dat er wordt gecontroleerd. Een voorbeeld van zo'n controlemaatregel is een registratie van vermiste goederen. Organisaties die een dergelijke registratie bijhouden zullen doorgaans sneller op het spoor komen van mogelijke verduisteringen dan bedrijven waarin een dergelijke registratie ontbreekt. Tegelijkertijd kan het bijhouden van een dergelijke registratie preventief werken, doordat werknemers de kans op betrapping hoger inschatten. Als beide effecten in enigerlei mate optreden, zullen monitoringsmaatregelen tegelijkertijd ertoe leiden dat meer zicht bestaat op mogelijke interne normovertredingen, terwijl de kans erop juist geringer is.
In blok 4 wordt gevraagd naar concrete normovertredingen waarvan het bedrijf in de afgelopen drie jaar slachtoffer is geworden. De periode van drie jaar is gekozen om voldoende respons te genereren en om ook ten aanzien van de minder frequent voorkomende vormen van criminaliteit te kunnen vaststellen welke problemen bedrijven zoal ervaren en hoe ze daar mee omgaan.
Bij het doorlopen van de lijst van mogelijke normovertredingen wordt in eerste instantie geen onderscheid gemaakt tussen externe en interne vormen van criminaliteit. Door eerst naar alle incidenten te vragen en vervolgens door te vragen naar mogelijke interne betrokkenheid bij deze incidenten, krijgen we zicht op de relatieve omvang van het probleem van interne criminaliteit, in relatie tot externe criminaliteit. Ook kunnen we zo beter nagaan wat de mogelijkheden en moeilijkheden zijn die bedrijven ervaren bij het vaststellen van interne (betrokkenheid bij) normovertredingen. Ten slotte verkleint deze benadering de kans dat respondenten incidenten vergeten te melden, omdat er slechts sprake is van een *vermoeden* van interne betrokkenheid.
De selectie van vijftien normovertredingen in de vragenlijst is gebaseerd op responspercentages die bij eerder onderzoek zijn aangetroffen. Dit verklaart waarom een zware nadruk ligt op incidenten in de vermogenssfeer (Cools, 1994). Overigens geldt voor deze lijst dat geen volledigheid is nagestreefd. In een vervolgvraag kunnen bedrijven aangeven of ze ook slachtoffer zijn geworden van andere dan de genoemde normovertredingen. De volgorde van de incidenten is hiërarchisch, bijvoorbeeld inbraak gaat in de vragenlijst vooraf aan verduistering, dat weer voorafgaat aan opzettelijke vernieling. Dit betekent dat een gebeurtenis die is gekwalificeerd als inbraak, later niet nog eens kan worden geteld als verduistering of als vernieling. Zulks om dubbeltellingen te voorkomen en een eenduidige toekenning van labels aan gebeurtenissen te bevorderen. Overigens blijft het altijd mogelijk dat incidenten zich afspelen op het grensvlak van twee categorieën. We hebben ervoor gekozen tijdens de interviews zoveel mogelijk het noemen van labels (zoals inbraak, fraude, corruptie, et cetera) te vermijden. In plaats daarvan worden de normovertredingen beschreven in termen van gedragingen. Dit om te voorkomen dat er misverstanden ontstaan doordat respondenten niet dezelfde inhoud toekennen aan de labels als de onderzoekers.

Ten slotte kan in dit verband nog iets worden gezegd over het onderscheid tussen *concrete* en *vermoedelijke* normovertredingen. De laatste categorie is vaak van toepassing bij interne criminaliteit. Wanneer bijvoorbeeld goederen zijn beschadigd, kan niet altijd worden aangetoond dat dit met opzet is gebeurd. Of er ontbreken bijvoorbeeld goederen, maar onduidelijk is of sprake is van verduistering, verkeerd laden, onachtzaamheid, et cetera. Het onderdeel van blok 4 waarin de vijftien normovertredingen staan vermeld, beoogt incidenten in kaart te brengen, die door de bedrijven als concrete of vermoedelijke normovertredingen worden gelabeld. De verwachting was echter dat de nadruk hierbij vooral zou liggen op concrete normovertredingen. Daarom zijn ook enkele aanvullende vragen opgenomen over vermoedelijke en mogelijke interne normovertredingen (*dark number* problematiek).
Indien een bedrijf in de afgelopen drie jaar éénmaal of vaker slachtoffer is geworden van enige vorm van criminaliteit (intern of extern), zijn aan de respondent enkele vervolgvragen voorgelegd, welke te vinden zijn in het aanhangsel van de vragenlijst dat als bijlage 2 is toegevoegd aan dit rapport ('Uitwerking normovertredingen'). Als bij één of meer van de genoemde incidenten sprake is van concrete óf vermoedelijke interne betrokkenheid, zijn over het laatste incident dat heeft plaatsgevonden nog enkele vervolgvragen gesteld. Deze hebben betrekking op de wijze waarop het incident (en mogelijk ook de dader) in het bedrijf bekend is geworden, en de manier waarop het bedrijf erop heeft gereageerd. Ook gaan we hierbij in op de achtergrondkenmerken van de eventuele verdachten.
In blok 5 is een aantal vragen opgenomen over de eventuele gang van bedrijven naar het strafrecht en de overwegingen die hierbij een rol spelen, bijvoorbeeld bij het doen van aangifte bij de politie. Tevens wordt hier gevraagd of bedrijven op de hoogte zijn van wat er met hun aangiften is gebeurd.
In blok 6 wordt de respondent de ruimte geboden nog enige aanvullende opmerkingen te maken. In blok 7, ten slotte, noteert de interviewer opvallende aspecten uit het interview.

1.5.3 Deskundigenraadpleging en aangiftenonderzoek

Deskundigenraadpleging
Zoals hiervoor al werd gemeld zijn naast de interviews bij bedrijven ook verschillende experts geïnterviewd (zie bijlage 3).
Enkele interviews zijn uitgevoerd om onze kennis te vergroten voor het samenstellen van de vragenlijst. Daarnaast hebben we na afloop van de interviews bij bedrijven gesproken met verschillende personen en instellingen die ons, vanuit een ander perspectief dan dat van de betrokken bedrijven, zicht konden bieden op enkele relevante kwesties. De selectie van deze respondenten is tot stand gekomen naar aanleiding van bevindingen in het hoofdonderzoek. De nadruk ligt hierbij op respondenten die kennis hebben van de opsporing van interne criminaliteit (en die dus ook 'daderkennis' hebben). Hierbij kan het gaan om private en politiële opsporingsinstanties. Omdat deze expertinterviews vooral zijn gebruikt ter validering van en ter aanvulling op de interviews bij bedrijven, zullen we de uitkomsten ervan niet apart bespreken. Waar dit aan de orde is, zullen we er wel melding van maken.

Vervolgonderzoek aangiften
Om te onderzoeken wat er gebeurt met de aangiften van bedrijven bij de politie (en later mogelijk ook bij justitie), hebben we een bevraging bij deze instanties uitgevoerd.
In de eerste plaats hebben we bij de bedrijven zoveel mogelijk gegevens verzameld omtrent aangiften van strafbare feiten waarbij concreet of vermoedelijk sprake is van interne betrokkenheid. Als het gaat om bedrijven met meerdere vestigingen, hebben we een overzicht gemaakt van de vestigingslocaties per bedrijf. Hierbij hebben we ons beperkt tot vestigingen waarover we met de respondenten hebben gesproken. Van deze vestigingen is vervolgens bepaald in welke politieregio deze gelegen zijn. Het gaat in totaal om circa 350 vestigingen.[5]

[5] Onze gegevens zijn meestal niet fijnmazig genoeg om in bedrijven met meerdere vestigingen te bepalen waar, dat wil zeggen in welke vestiging, een incident heeft plaatsgevonden. Om die reden hebben we de aangiften van álle vestigingen opgevraagd.

Aansluitend zijn alle politieregio's in Nederland benaderd waar vestigingen vóórkomen van bedrijven uit onze steekproef. Aan deze regio's is gevraagd of zij van de genoemde bedrijven aangiften hebben ontvangen in de periode 2002-2004 en zo ja, welke (door ons geselecteerde) kenmerken deze aangiften hebben. Hierbij hebben we geen selectie gemaakt op interne betrokkenheid, maar gevraagd naar alle aangiften van de betrokken bedrijven. De reden hiervoor is dat interne betrokkenheid niet altijd kan worden afgeleid uit de aangifte, terwijl wij via de bedrijven soms weten dat hiervan (waarschijnlijk) wel sprake is. Wel hebben we de politieregio's gevraagd om aan te geven of uit de aangifte blijkt dat (mogelijk) sprake is van interne betrokkenheid. We hopen hiermee extra interne aangiften te vinden die niet door de bedrijven zijn gemeld.[6] Na afloop van de bevraging bij de politie hebben we de verzamelde gegevens waar mogelijk aangevuld met gegevens die bedrijven ons verstrekt hebben. Hierbij gaat het vooral om het identificeren van interne betrokkenheid bij aangiften, zodat we deze als aparte categorie kunnen behandelen in het verdere onderzoek.
Uit de verzamelde gegevens zijn de interne aangiften geselecteerd die hebben geleid tot een voorgeleiding van één of meer verdachten aan de Officier van Justitie. Ten slotte is bij het Centraal Justitieel Documentatiesysteem in Almelo nagegaan of deze verdachten zijn vervolgd en welke veroordeling hierop eventueel is gevolgd.
Op basis van deze gegevens kunnen we uitspraken doen over de concrete politiële en justitiële *follow up* bij aangiften van interne criminaliteit.

[6] Het is niet ons doel om de opgaven van de politie naast die van de bedrijven te leggen om te kijken in hoeverre bedrijven aangiften hebben gemeld die niet kunnen worden teruggevonden bij de politie of in hoeverre aangiften worden gevonden bij de politie die niet zijn gemeld door bedrijven. Een dergelijke check valt buiten het bestek van dit onderzoek. Het is ons hier vooral te doen om zoveel mogelijk interne aangiften te vinden.

2 Beschrijving van de bedrijven en respondenten

In dit hoofdstuk bespreken we de steekproefsamenstelling en de respondenten waarmee wij hebben gesproken. Achtereenvolgens zullen wij daartoe in paragraaf 2.1 behandelen hoe deze steekproef tot stand is gekomen en in paragraaf 2.2 hoe de steekproef is samengesteld. In paragraaf 2.3 bespreken we welke respondenten wij hebben geïnterviewd en hoe het verloop van de interviews eruit zag. In paragraaf 2.4 bespreken we ten slotte kort de samenvatting en conclusie.

Terminologie
Vooraf dient opgemerkt te worden dat wij de term 'steekproef' hier gebruiken om de groep van bedrijven aan te duiden die heeft meegewerkt aan dit onderzoek. Feitelijk heeft er geen steekproeftrekking plaatsgevonden, omdat alle bedrijven uit de (operationele) populatie zijn benaderd.

2.1 Totstandkoming steekproef

Bij het benaderen van bedrijven hebben wij gebruik gemaakt van bronnen van verschillende brancheorganisaties. Hiermee konden wij die logistiek dienstverleners benaderen voor wie enige vorm van *warehousing* (eventueel in combinatie met *value added logistics*) een kernactiviteit vormt. TLN en EVO stelden hun ledenlijsten niet beschikbaar voor onderzoek.[7] De Physical Distribution Group (PDG), een aantal logistiek dienstverleners dat zich heeft verenigd onder de mantel van TLN, deed dit wel.[8] Ook de ledenlijsten van NDL en Fenex waren beschikbaar.[9] Voor NDL geldt dat hierbij naar eigen zeggen 80 á 90% van de internationaal opererende logistiek dienstverleners is aangesloten. Daarnaast beschikken regionale handelscentra soms over overzichten van lokaal actieve bedrijven. Zo geeft de website van de haven van Rotterdam een overzicht van alle bedrijven die daar aan *warehousing* doen en doet het Five Mode Distri Network (5MDN) dit voor de regio Arnhem - Nijmegen.[10] En andere goede bron is de Top 150 Logistiek Dienstverleners (LDV's) van de LogistiekKrant.[11] Al met al levert dit het volgende overzicht op:

Fenex ledenlijst	Specialisatie: opslag en distributielogistiek	117 bedrijven
NDL Ledenlijst	LDV's met opslag LDV's met opslag en VAL	157 bedrijven
Port of Rotterdam	LDV's met *warehousing* LDV's met *warehousing* gevaarlijke stoffen	133 bedrijven
TLN	LDV's uit de Physical Distribution Group	53 bedrijven
LogistiekKrant	Top 150 LDV's met uitzondering van de bedrijven die niet aan *Warehousing*/VAL doen	149 bedrijven
5MDN Ledenlijst	Specialisatie: VAL	22 bedrijven

In totaal komen wij met deze bronnen op 631 bedrijfsnamen. Na ontdubbeling van bedrijven die op meer dan één lijst voorkwamen, blijven er 353 bedrijven over. Volgens diverse deskundigen die wij hebben geraadpleegd, kunnen deze 353 bedrijven worden beschouwd als zijnde de kern van de

[7] Zie voor meer informatie: www.tln.nl en www.evo.nl.
[8] Zie voor meer informatie: www.pdg.nl.
[9] Zie voor meer informatie: www.ndl.nl en www.fenex.nl.
[10] Zie voor meer informatie: www.portofrotterdam.com en www.5mdn.nl.
[11] zie voor meer informatie: http://www.zibb.nl/logistiek/dossier.asp?dossier=742.

logistieke dienstverlening in Nederland. Sommigen schatten dat deze bedrijven zo'n beetje de gehele populatie vormen. Uitgaande van een verwachte respons van om en nabij de 50% en ook rekening houdend met de mogelijkheid dat de populatie van 353 mogelijk vervuild is met bedrijven die niet aan ons selectiecriterium voldoen (kernactiviteit *warehousing*/VAL), heeft er géén steekproeftrekking plaatsgevonden. Met andere woorden, we hebben de gehele populatie benaderd.
Eind september 2004 is begonnen met het benaderen van respondenten voor interviews. Van de lijst met 353 bedrijven bleken 68 niet te voldoen aan het selectiecriterium (kernactiviteit *warehousing*). In de meeste gevallen ging het hierbij om bedrijven die de *warehousing* activiteiten hadden uitbesteed of een holdingfunctie vervulden. In totaal 146 bedrijven hebben laten weten niet mee te willen werken (te druk, geen belang, et cetera).[12] Met de overige 139 bedrijven zijn interviews gerealiseerd (door een late afzegging haalden wij niet ons streefaantal van 140 bedrijven). Eind december 2004 hebben wij deze interviews afgerond. In onderstaand overzicht zijn de gegevens op een rij gezet.

Onzuivere populatie (bedrijven op ledenlijsten van brancheorganisaties)	353
Bedrijven die niet aan populatiecriteria bleken te voldoen	68 –
	===
Zuivere populatie (bedrijven met kernactiviteit *warehousing*/VAL)	285
Weigeringen/niet kunnen bereiken/onbruikbare interviews	146 –
	===
Steekproef (bedrijven in onderzoek)	139 (49%)

Hiermee blijken wij zeer dicht bij de door ons van tevoren ingeschatte respons te zitten. Wel hebben wij hiervoor alle 353 bedrijven moeten benaderen. Verschillende factoren dragen ertoe bij dat de respons lager uitvalt dan mogelijk was geweest. Enerzijds is de periode voor de decembermaand voor veel bedrijven de drukste periode van het jaar. Potentiële respondenten gaven aan hierdoor, meer dan op andere momenten in het jaar, geen tijd voor ons te hebben. Anderzijds ondervonden wij hinder van enige parallel lopende onderzoeken. Verschillende bedrijven bleken in dezelfde periode te zijn aangeschreven of gebeld over
aanverwante thema's. Zo zijn we geconfronteerd met een (telefonisch) onderzoek van het NIPO (in opdracht van het ministerie van Justitie) naar criminaliteitservaringen van bedrijven (Monitor Bedrijven en Instellingen 2004), een onderzoek van de PDG naar verzekerbaarheid van risico's in de logistieke sector en een onderzoek van het ministerie van VROM naar milieucriminaliteit. Gegeven deze omstandigheden zijn we niet ontevreden over de respons.

2.2 Samenstelling steekproef

In totaal hebben wij uiteindelijk bij 139 bedrijven een interview afgenomen. De bedrijven zijn op verschillende manieren in te delen. Zoals wij al in hoofdstuk 1 hebben aangegeven, kiezen wij ervoor dit te doen naar aanleiding van: 1) aantrekkelijkheid van doelwitten, 2) omvang van de onderneming en 3) regionale/stedelijke ligging. Wij bespreken deze hier één voor één en gaan vervolgens na in hoeverre de samenstelling van de steekproef verschilt van die van de populatie.

Aantrekkelijkheid van doelwitten
Het spreekt voor zich dat een bedrijf dat doet in papier en verpakkingen niet dezelfde risico's loopt als een bedrijf dat consumentenelektronica opslaat. We hebben alle bedrijven in ons onderzoek daarom ingedeeld in één van de volgende drie klassen: goederen met een laag, middelgroot of groot risico. De toekenning is in zekere zin arbitrair, maar volgt in grote lijnen de risico-indelingen die ook door verzekeraars worden gebruikt (TLN, 2003). Als meest risicovol zijn 79 bedrijven (57%) gecategoriseerd. Zij doen in waardevolle en goed verhandelbare consumentengoederen, zoals consumentenelektronica, pc's en toebehoren, witgoed, huishoudelijke apparaten, auto-onderdelen,

[12] Hierbij dient te worden opgemerkt dat wij bij 6 bedrijven helemaal geen contact met de beoogde respondent hebben kunnen krijgen.

merkkleding, persoonlijke-verzorgingsproducten (zoals parfum en dergelijke), sterke drank, sigaretten en dergelijke. Een middelgroot risico lopen 53 bedrijven (38%). Zij be- of verwerken de overige (minder waardevolle) consumentengoederen, zoals levensmiddelen, speelgoed en andere *non-food*artikelen, maar ook hoogwaardige industriële producten en chemische, farmaceutische en medische producten. Ten slotte worden 7 bedrijven (5%) met een laag risico onderscheiden: zij werken met laagwaardige of lastig transporteerbare goederen zoals papier, bulkgoederen en dergelijke. Een bedrijf dat altijd hoogwaardige consumentenelektronica vervoert, zou eigenlijk in een hogere categorie moeten worden ingedeeld dan een bedrijf dat dit sporadisch doet. Dit onderscheid is op basis van onze gegevens echter lastig te maken. Als bedrijven in verschillende goederen handelden, is de categorisering van het betreffende bedrijf daarom afgestemd op de meest risicovolle goederen waarmee men werkte.

Omvang van ondernemingen
Voor wat betreft de omvang van de bedrijven kunnen we op twee manieren een onderscheid maken: op basis van de omzet in 2003 en op basis van het aantal werknemers in Nederland. Aangezien respondenten over het algemeen meer zicht hadden op het aantal werknemers dan op de precieze omzet (van de vestiging, van het bedrijf, nationaal of internationaal), gebruiken wij het aantal werknemers als indicator om de bedrijven in te delen in klein (27%), middelgroot (38%) en groot (35%). Kleine bedrijven hebben minder dan vijftig werknemers; middelgrote bedrijven hebben vijftig tot tweehonderd werknemers in dienst; en grotere bedrijven tellen meer dan tweehonderd personeelsleden. Door de variabele omvang (op basis van personeel) te valideren door naar de gemiddelde omzet van die bedrijven te kijken, blijken deze bedrijven een gemiddelde omzet van respectievelijk 5, 22 en 389 miljoen euro te hebben. Het aantal werknemers is dus een geschikte variabele om de omvang van bedrijven in te schatten.

Locatie van bedrijven
Een andere indeling die wij kunnen maken is die gebaseerd op locatie. Grotere bedrijven hebben echter verschillende vestigingen in het hele land (en eventueel daarbuiten). Onze respondenten bij deze vestigingen waren steeds verantwoordelijk voor één of meer van deze vestigingen. Het toekennen van een locatie aan een bedrijf is gebaseerd op de locatie van de hoofdvestiging van het bedrijf, zijnde de locatie die wij (meestal) hebben bezocht. Dit is in zekere zin een arbitraire toekenning, waarbij een rol heeft gespeeld dat de respondenten vaak de meeste kennis hadden over de vestiging of vestigingen waar ze zelf verbleven. Deze vestigingslocaties hebben wij vervolgens ingedeeld in vijf verschillende regio's waar zich concentraties van bedrijven bevinden: 29 bedrijven (21%) in Rotterdam en omgeving, 15 bedrijven (11%) op en rond Schiphol, 20 bedrijven (14%) in de rest van de randstad, 42 bedrijven (30%) in Noord-Brabant/Limburg en 33 bedrijven (24%) verspreid over de rest van Nederland.
Tevens kunnen wij nog een aantal andere onderverdelingen maken. Zo kunnen wij bedrijven bijvoorbeeld ook indelen op bewerkingen, aandeel extern transport, certificering en verloop van het personeel. Deze en de hiervoor genoemde indelingen zijn vastgelegd in tabel 1.

Tabel 1 Gegevens over de bedrijven in %

Geografische ligging (n=139)	*Aard bedrijfsactiviteiten: % loodspersoneel (n=137)*
Regio Schiphol (11%)	0-25 procent (21%)
Regio Rotterdam (21%)	26-50 procent (26%)
Overige randstad (14%)	51-75 procent (14%)
Noord-Brabant/Limburg (30%)	76-100 procent (39%)
Elders in Nederland (24%)	
Aard bedrijfsactiviteiten: transportfunctie	*Bewerkingen op producten (n=137)*

(n=134)

Geen transport/uitbesteed (65%)	Alleen op- en overslag goederen (7%)
Wel transport/deels uitbesteed (35%)	Bewerking van goederen/VAL (93%)

Risicovolle goederen (n=139)	*Omvang (in Nederland) (n=139)*
Producten met laagste risico (5%)	Klein: < 50 werknemers (27%)
Producten met middelgroot risico (38%)	Middelgroot: 50-200 werknemers (38%)
Producten met grootste risico (57%)	Groot: > 200 werknemers (35%)

Monitoren kwaliteit van leveringen (n=136)	*Certificering (n=138)*
Gebeurt niet (22%)	TAPA (14%)
Gebeurt wel (78%)	ISO/anders (53%)
	Niet (33%)

Aanwezigheid van extern personeel in bedrijf (n=128)	*Problemen met werven van 'goed' personeel (n=135)*
Geen extern personeel aanwezig (13%)	Geen problemen (41%)
Wel extern personeel aanwezig (87%)	Wel problemen (59%)

Non-respons analyse

Het is mogelijk gebleken om ook voor de meeste van de 146 bedrijven die niet wilden meewerken de hiervoor genoemde kenmerken (globaal) in kaart te brengen. Door de gerealiseerde steekproef van 139 bedrijven op deze kenmerken te vergelijken met de populatie van 285 bedrijven, kunnen we verschillende zaken signaleren.

Aangezien slechts 4 bedrijven op Schiphol niet wilden meewerken, ligt de non-respons daar gemiddeld veel lager dan in de andere regio's (18%). Ook 56 bedrijven in Rotterdam (non-respons 67%), 21 bedrijven in de rest van de randstad (non-respons 54%), 30 bedrijven in Noord-Brabant en Limburg (non-respons 42%) en 35 bedrijven in de rest van Nederland (non-respons 51%) wensten geen medewerking te verlenen. Daarmee ligt de respons het laagst in Rotterdam en verreweg het hoogst rond Schiphol. De hoge respons op Schiphol is deels te verklaren uit het feit dat wij daar meer moeite hebben gedaan om bedrijven 'binnen te halen' (de verwachting vooraf was dat de nonrespons hier juist hoger zou liggen). De lage respons in Rotterdam is lastiger te verklaren. Een relatief groot deel van de bedrijven is van kleine omvang (dus: doorgaans weinig problematiek). Ook is een deel van deze bedrijven relatief laat benaderd, waardoor het effect van de aanbevelingsbrief mogelijk minder groot is geweest. Ook hebben we bij deze bedrijven (naar verhouding) minder moeite gedaan om ze tot medewerking over te halen, omdat het steekproefquotum bijna was bereikt.

Kijken we naar de omvang van de bedrijven, dan hebben wij daar voor 84 van de 146 non-respons bedrijven een redelijk zicht op. Van deze bedrijven zijn 22 klein, 44 middelgroot en 18 groot. De non-respons onder de grote bedrijven is dus kleiner (44%) dan onder de middelgrote (59%) en kleine (50%) bedrijven. Hierbij moet wel een kanttekening worden geplaatst. Wij hebben redenen om aan te nemen dat de bedrijven waarvoor wij geen zicht hadden op de omvang, relatief kleiner zullen zijn geweest.[13] Waarschijnlijk is daarom in werkelijkheid de non-respons onder kleine bedrijven groter en onder grote bedrijven kleiner dan deze cijfers doen vermoeden.

[13] Immers, grotere bedrijven zullen eerder op een van de lijsten van NDL, PDG, 5MDN of de Top 150 Logistiek Dienstverleners voorkomen (al deze lijsten geven inzicht in de omvang van de bedrijven en het soort goederen dat zij verwerken).

Wat betreft het soort goederen kunnen wij van 77 van de 146 bedrijven aangeven met welke goederen zij zich bezig houden. Slechts 5 bedrijven doen in bulkgoederen of vloeistoffen (non-respons 59%). Een groter aantal bedrijven (26) zit in het middensegment (non-respons 48%) en 46 bedrijven werken onder andere met hoogwaardige goederen (non-respons 52%). De respons onder bedrijven met laagwaardige goederen ligt iets lager omdat zij relatief minder vaak de noodzaak zagen om aan het onderzoek mee te werken.

Samenvattend kunnen wij stellen dat er verschillen zijn tussen de samenstelling van de populatie en de steekproef. Grotere bedrijven vielen relatief minder vaak af dan kleinere. Daarnaast was de respons op Schiphol (waar zich veel grote bedrijven bevinden) veel hoger dan die rond Rotterdam.

2.3 Respondenten en verloop van interviews

Medio september 2004 is gewerkt aan de constructie van de vragenlijst. Ter voorbereiding hierop hebben we een viertal interviews afgenomen bij deskundigen in het veld om ons een beeld te vormen van relevante thema's en de wijze waarop deze in de vragenlijst aan de orde kunnen komen. We hebben in dit kader gesproken met:

- De secretaris Criminaliteitsbeheersing van de ondernemingsorganisatie VNO-NCW (tevens voorzitter van werkgroep negen van het voornoemde Actieplan Veilig Ondernemen, de werkgroep die zich bezighoudt met het aandachtsveld 'Aanpak interne criminaliteit');
- De juridisch beleidsmedewerker van Transport en Logistiek Nederland die ook criminaliteitsbeheersing in haar portefeuille heeft;
- De *security* manager Benelux van een grote logistiek dienstverlener (Exel);
- Een risicoconsultant op het gebied van bedrijfsbeveiliging die is gespecialiseerd in de logistieke sector (Reijenga Risk Management).

De vragenlijst is in concept voorgelegd aan de begeleidingscommissie en bij enkele bedrijven getest, waarna de definitieve vragenlijst is vastgesteld (zie bijlagen 1 en 2). Deze vragenlijst hebben wij afgenomen bij respondenten op de locatie van de bedrijven. De interviews bij bedrijven werden afgenomen door de betrokken onderzoekers, een onderzoeksassistent en een veldwerker.
De respondenten van de bedrijven zijn ook in te delen in verschillende groepen. Zo kunnen wij de functie van de respondent onderscheiden, het aantal jaren dat hij of zij in functie is, de vorige werkkring en het aantal uren dat aan het thema *security* wordt besteed. Dit onderscheid is opgenomen in tabel 2.

Tabel 2 Gegevens over de respondenten in % (n=139, tenzij anders vermeld)

Functie	*Uren besteed aan* security *(n=137)*
Security manager (12%)	Fulltime (9%)
Kwaliteitsmanager (18%)	10 tot 30 uur per week (9%)
Directeur (31%)	Minder dan een dag per week (82%)
Operationaal/logistiek/*facility* manager (18%)	
Overig (21%)	
Aantal jaren dat functie wordt bekleed	*Vorige werkkring (n=137)*
Meer dan 5 jaar (42%)	Logistiek (74%)
2 t/m 5 jaar (35%)	Beveiliging/politie (5%)

Minder dan 2 jaar (23%) Management (9%)

Anders (12%)

De kennis die respondenten hebben, blijkt nogal te variëren. Dit hangt onder andere samen met de omvang van de onderneming, de functie van de respondent en de vestiging(en) waarop deze zicht heeft. Zoals hiervoor al genoemd, kwam het soms voor dat we een functionaris interviewden die verantwoordelijk was voor de beveiliging van een bedrijf met bijvoorbeeld vijf vestigingen in Nederland, terwijl deze persoon slechts zicht had op de vestiging(en) waar hij/zij zelf vaak verbleef. Ook de functie is van belang: hoe meer een respondent is gespecialiseerd in beveiligingsaangelegenheden, des te groter is doorgaans zijn/haar kennis van wat zich op dit vlak afspeelt in het bedrijf. Ook het aantal jaar ervaring in functie is hierop van invloed. Bijna een kwart van de respondenten (23%) kan bijvoorbeeld geen volledig zicht hebben over de afgelopen drie jaar omdat hij/zij minder dan twee jaar in dienst was. Dit zal zeker van invloed zijn geweest op het aantal gerapporteerde incidenten. Over met name de kleinere incidenten van voor hun aanstelling zullen zij minder hebben geweten.
Behalve de respons van bedrijven, is ook de bereidwilligheid van respondenten om te praten over kwesties betreffende interne criminaliteit en beveiliging binnen hun bedrijven bevredigend. Bij circa twintig respondenten signaleerden wij enige terughoudendheid en sociaal gewenst antwoordgedrag. In achttien gevallen bleek de respondent niet op alle vlakken even deskundig. Gemiddeld genomen waren de respondenten echter open over wat zich in de bedrijven afspeelt. De waarborgen van vertrouwelijkheid die we de respondenten hebben geboden, lijken derhalve afdoende te hebben gewerkt.
Ten slotte hebben wij gebruik gemaakt van elf open expertinterviews om op een kwalitatieve manier onze conclusies te controleren, te ondersteunen en aan te vullen. We hebben in dit kader gesproken met:

- Een medewerker van het Landelijk Team Transportcriminaliteit (LTT) van het Korps Landelijke Politiediensten (KLPD). Dit is een expertisecentrum waar alle meldingen over trailer- en ladingdiefstal binnenkomen. Deze kennis wordt veredeld en vervolgens beschikbaar gesteld aan opsporingsteams bij de politie;
- Een medewerker van het Boven Regionaal Team (BRT) van de politie in Zuid-Nederland. Dit team heeft in het recente verleden vijf opsporingsonderzoeken uitgevoerd naar ladingdiefstal in Zuid-Nederland (waar deze diefstal het meest vóórkomt);
- Het hoofd Opsporing van de Zeehavenpolitie in Rotterdam (veel van de bedrijven in ons onderzoek zijn in dit gebied gelokaliseerd);
- De chef Recherche van de Zeehavenpolitie in Rotterdam en tevens medewerker van het Expertisecentrum Haven. Dit is een multidisciplinaire eenheid die zich richt op de opsporing van georganiseerde criminaliteit in de Rotterdamse haven (in dit centrum wordt samengewerkt met organisaties als de Douane, de FIOD-ECD[14], de Nationale Recherche en de Zeehavenpolitie);
- Twee rechercheurs Bedrijfscriminaliteit van de Koninklijke Marechaussee (KMar) op Schiphol. De KMar is op Schiphol belast met de opsporing van strafbare feiten;
- Een project manager van Hoffmann Bedrijfsrecherche, het grootste bureau voor private bedrijfsrecherche in Nederland;
- Twee medewerkers van Ernst & Young Integrity Services & Investigations die gespecialiseerd zijn in transport en logistiek (preventie, risicoanalyse, schadeonderzoek).

Daarnaast zijn we gericht op zoek gegaan naar aanvullende informatie over verzekeringskwesties. In dit verband hebben we gesproken met:

[14] De FIOD-ECD (Fiscale Inlichtingen- en Opsporingsdienst/Economische Controledienst) is de opsporingsdienst van de Belastingdienst.

- De secretaris van de Physical Distribution Group (PDG), een belangengroep van ruim vijftig doorgaans grotere logistiek dienstverleners (de respondent heeft recentelijk een onderzoek naar verzekeringskwesties uitgevoerd onder de leden van de PDG);
- Twee medewerkers van Aon Nederland (dienstverlener op het gebied van assurantiën en risicomanagement) die zijn gespecialiseerd in de logistieke sector. We hebben hier gesproken met een makelaar in assurantiën (iemand die polissen voor bedrijven maakt) en met een risicoconsultant.

Voorts hebben we gesproken met vertegenwoordigers van opdrachtgevers die logistiek dienstverleners inschakelen (de verladers):

- Een beleidsmedewerker van de afdeling Criminaliteitsbeheersing van verladersorganisatie EVO;
- De *security* manager van HP EMEA (Elektronicaconcern), tevens vice-voorzitter van TAPA EMEA (Technology Asset Protection Association). TAPA is een samenwerkingsverband van elektronicaproducenten die een beveiligingscertificaat hebben ontwikkeld waaraan logistiek dienstverleners moeten voldoen als zij voor deze bedrijven opdrachten willen uitvoeren.

Ten slotte hebben we ook gesproken met:

- De voorzitter van het Kenniscentrum Criminaliteitspreventie van Air Cargo Netherlands (ACN). ACN is een belangenorganisatie voor de luchtvrachtindustrie op Schiphol (waar veel van de bedrijven uit ons onderzoek zich bevinden). Recentelijk zijn vanuit het Regionaal Platform Criminaliteitsbeheersing nieuwe initiatieven ontwikkeld om de veiligheid voor bedrijven op Schiphol te vergroten. De respondent vervult in deze ontwikkelingen een sleutelrol en is jarenlang in verschillende functies betrokken geweest bij grote luchtvrachtafhandelaren.

In totaal hebben wij bij 139 bedrijven de vragenlijst afgenomen en gebruik gemaakt van vijftien aanvullende expertinterviews.

2.4 Samenvatting en conclusie

Met 139 gerealiseerde interviews zitten wij vlakbij de geschatte respons van 50%. De bedrijven vertonen een redelijk goede spreiding als het gaat om omvang, locatie en de hoogwaardigheid van de goederen. Het is niet vreemd dat relatief minder bedrijven met laagwaardige goederen in de steekproef zitten. Hiervan zijn er minder en wilden er minder meewerken (vanwege vermeende irrelevantie). Opvallend is wel dat een relatief groot aantal bedrijven uit de Rotterdamse regio niet wilde meewerken (dit zijn ook vaak kleine bedrijven). De kennis van respondenten was over het algemeen vrij goed. Enkele keren waren zij niet op alle gebieden even deskundig of vertoonden zij sociaal gewenst antwoordgedrag. Samenvattend kunnen wij concluderen dat de bedrijven een redelijke doorsnede vormen van de onderzochte sector, met uitzondering van de kleine bedrijven in Rotterdam (die *onder*vertegenwoordigd zijn) en de grote bedrijven op Schiphol (die *over*vertegenwoordigd zijn).

3 Aard en omvang van interne criminaliteit bij logistiek dienstverleners

In dit hoofdstuk beschrijven we onze bevindingen ten aanzien van onderzoeksvragen 1 en 3.

- *Wat is de aard en omvang van de interne criminaliteit waarmee logistiek dienstverleners in de afgelopen drie jaar zijn geconfronteerd?*
- *Op welke wijze zijn de genoemde voorvallen van interne criminaliteit aan het licht gekomen en in hoeverre bestaan er binnen de bedrijven belemmeringen om een goed zicht op dit verschijnsel te hebben?*

In de navolgende paragrafen geven we een overzicht van de belangrijkste bevindingen. In paragraaf 3.1 behandelen we de terminologie en verschillende meetkwesties. In paragraaf 3.2 presenteren we de cijfers omtrent aard en omvang van (interne) criminaliteit. In paragraaf 3.3 gaan we in op de schade die bedrijven ondervinden van (interne) criminaliteit. In paragraaf 3.4 verdiepen we het empirisch materiaal door meer in detail te bespreken met welke -interne- problemen bedrijven te maken hebben en hoe deze aan het licht komen. In paragraaf 3.5 gaan we nader in op de onderrapportageproblematiek en de wijze waarop deze de bevindingen beïnvloedt. In paragraaf 3.6 vergelijken we de bevindingen met de resultaten uit eerder onderzoek. Het hoofdstuk besluit met een samenvatting en conclusie (paragraaf 3.7).

3.1 Terminologie en meetkwesties

Alvorens over te gaan tot de beschrijving van de onderzoeksresultaten, lichten we kort enkele zaken toe.

3.1.1 Gebruikte terminologie

In deze studie staan interne normovertredingen centraal. Dit zijn gedragingen die deels te betitelen zijn als criminaliteit, maar deels ook niet. Ter voorkoming van omslachtig taalgebruik zullen we hierna in samenvattende zin soms spreken over interne criminaliteit. De lezer dient zich te realiseren dat hiermee niet alleen gedragingen worden bedoeld die strafbaar zijn gesteld in het Wetboek van Strafrecht of enig ander wetboek. Tijdens de bevraging van de bedrijven is zoveel mogelijk vermeden om de normovertredingen te labelen. We hebben de gedragingen omschreven en aan de respondenten gevraagd in hoeverre bedrijven hiermee in de afgelopen drie jaar te maken hebben gehad (zie bijlage 1, de vragenlijst: blok 4). Ten behoeve van deze rapportage hebben we de verschillende normovertredingen van een label voorzien. Deze labels moeten worden beschouwd als een maatschappelijke (in plaats van een strafrechtelijke of juridische) classificatie. In schema 1 geven we aan aan welke 'inhoud' (qua normovertredend gedrag) achter deze labels schuilgaat.[15]

Schema 1 Omschrijving van normovertredingen

Label	*Korte omschrijving*
Inbraak	Vorm van diefstal waarbij de daders een inspanning moeten leveren om zichzelf toegang te verschaffen tot de gewenste buit, bijvoorbeeld door middel van verbreking van deuren of ramen, het buiten werking stellen van een alarm, et cetera. Naast inbraak in gebouwen, kan het hierbij ook gaan om inbraak op bedrijfsterreinen en diefstal van en uit

[15] Het gebruik van (correcte) juridische classificaties is bij een onderzoek als het onderhavige niet haalbaar. Daarvoor ontbreekt het de meeste respondenten aan voldoende kennis van de (afzonderlijke) feiten en van de juridische classificaties als zodanig. De door ons gevolgde werkwijze (tijdens de interviews geen labels noemen, maar gedragingen omschrijven) levert naar onze mening de meest bruikbare data op.

	vrachtauto's (trailer-, lading- en cabinediefstal)
Verduistering	Personen die ongeoorloofd geld, goederen of andere zaken van het bedrijf wegnemen of zich toe-eigenen, waartoe zij door de uitoefening van hun werk toegang hebben (zonder hierbij gebruik te maken van braak of enige vorm van manipulatie, zoals valse opgaven of voorwendsels)
Verwijtbaar onprofessioneel handelen	Personen die verwijtbaar hebben gehandeld zonder dat hierbij sprake hoeft te zijn van opzet (bijvoorbeeld een medewerker die tegen de regels een hek open laat staan waardoor een inbraak kan plaatsvinden)
Verbaal of fysiek geweld	Personen die collega's pesten, lastigvallen, intimideren, bedreigen of fysiek geweld jegens hen uitoefenen
Fraude	Personen die administratieve opgaven hebben vervalst of niet naar waarheid hebben opgemaakt om zichzelf aldus te bevoordelen (bijvoorbeeld sjoemelen met vrachtbrieven of kostendeclaraties)
Oplichting	Personen die onder valse voorwendsels een bedrijf bewegen tot het beschikbaar stellen van geld, goederen of andere zaken (bijvoorbeeld door nepfacturen te sturen)
Overval	Personen die gebruik maken van (dreiging met) fysiek geweld teneinde bedrijfsmiddelen, geld of goederen buit te maken
Vernieling	Personen die opzettelijk schade toebrengen aan gebouwen, handelswaar, bedrijfsmiddelen of andersoortige zaken die het bedrijf bezit of beheert
Doorspelen bedrijfsinformatie	Personen die waardevolle en/of vertrouwelijke bedrijfsgegevens aan derden doorspelen zonder dat hierbij sprake is van een koppeling aan andere incidenten (dus niet: informatie doorgeven voor een inbraak)
Illegale handel	Personen die middelen van het bedrijf (zoals vrachtauto's) gebruiken voor de handel in illegale goederen of diensten (zoals drugs- en mensensmokkel)
Privé-gebruik bedrijfsmiddelen	Personen die ongeoorloofd middelen van het bedrijf gebruiken voor privé-doeleinden (zoals privé telefoongesprekken op kosten van de baas)
Sabotage van werkprocessen	Personen die opzettelijk reguliere bedrijfsprocessen in de war sturen, door bijvoorbeeld verkeerde afspraken te maken of door ongeoorloofd niet aanwezig te zijn
Corruptie	Personen die privé-voordelen genieten in ruil voor een gunst (een dienst of aanbesteding), waardoor het bedrijf financieel wordt benadeeld
Commerciële activiteiten ten eigen bate	Personen die ongeoorloofd middelen van het bedrijf gebruiken (zoals een transportmiddel of tijd van de baas), om op eigen titel en op commerciële basis inkomsten te verwerven

3.1.2 Meting van slachtofferschap van interne criminaliteit

In hoofdstuk 1 hebben we al gewezen op het feit dat het verschijnsel 'interne criminaliteit' een moeilijk te meten verschijnsel is. Dit komt omdat incidenten niet altijd zichtbaar worden en als ze al zichtbaar worden is niet altijd duidelijk of sprake is van interne betrokkenheid. Ook zal het zo zijn dat niet alle incidenten bij onze respondenten bekend zijn en als ze wel bekend zijn, willen ze misschien

niet altijd erover praten. Bovendien: het onderscheid tussen externe en interne criminaliteit en het onderscheid tussen criminaliteit en (bijvoorbeeld) onregelmatigheden in het werkproces (bijvoorbeeld mistellingen) is lang niet altijd duidelijk.
Vanwege deze problematiek hebben we ervoor gekozen de bevraging niet te beperken tot slachtofferschap van concrete incidenten van interne criminaliteit, maar de volgende drieslag te maken:

1 We hebben in eerste instantie gevraagd naar slachtofferschap van criminaliteit in het algemeen, dus alle concrete (externe en interne) incidenten die hebben plaatsgevonden;
2 Vervolgens hebben we de bedrijven die slachtoffer zijn geworden van de genoemde vorm van criminaliteit, gevraagd in hoeverre er concrete aanwijzingen of vermoedens zijn dat sprake is van interne betrokkenheid bij de genoemde incidenten;
3 Ten slotte hebben we, los van voornoemde concrete incidenten, aan de bedrijven gevraagd of zij het idee hebben dat er interne criminaliteit plaatsvindt waar zij géén of slecht zicht hebben en zo ja, waaruit dit zoal blijkt (onregelmatigheden in de bedrijfsvoering: voorraadverschillen, et cetera).

De ratio achter deze wijze van bevraging is dat we het verschijnsel interne criminaliteit op deze manier volledíger kunnen beschrijven. Door het te beschouwen als een onderdeel van alle concrete incidenten van criminaliteit waarmee het bedrijf te maken heeft, kunnen we eerder en beter zicht krijgen op mogelijk verborgen interne criminaliteit. Een zelfde redenering gaat op voor de bespreking van onregelmatigheden in de bedrijfsvoering.
Ter toelichting op de tweede stap: van concrete vermoedens van interne criminaliteit is sprake als de respondenten uit feiten en omstandigheden afleiden dat het waarschijnlijk of zeer waarschijnlijk is dat één of meer zijn internen betrokken bij de genoemde incidenten. Een kwalificatie als ‘het zou best kunnen’ is hiervoor te zwak.

3.1.3 Overige meetkwesties

In paragraaf 1.5.2 hebben we reeds uiteengezet dat bij de bevraging gebruik is gemaakt van een hiërarchische lijst van normovertredingen. Een incident dat eenmaal gelabeld is als een inbraak, kan derhalve daarna niet nog eens vóórkomen als een verduistering of een vernieling. Dit hebben we gedaan om dubbeltellingen te voorkómen en om de verschillende categorieën zo éénduidig mogelijk te ‘vullen’ met soortgelijke incidenten. In de praktijk doen zich wel eens gevallen voor, waarbij een medewerker tegelijkertijd diverse normovertredingen heeft begaan, waarbij het niet goed mogelijk is deze te labelen als afzonderlijke gebeurtenissen. In die gevallen is de beschrijving van betreffend gedrag terecht gekomen in de eerste van toepassing zijnde (incident)categorie.
In het verlengde hiervan het volgende: in sommige gevallen is sprake van een reeks gerelateerde gebeurtenissen die moeilijk afzonderlijk kunnen worden beschouwd, bijvoorbeeld een medewerker die twee jaar lang zeer regelmatig met onkostendeclaraties heeft geknoeid. In dit soort gevallen hebben we de reeks van gebeurtenissen geteld als één incident.
Het is mogelijk dat gebeurtenissen die sterk op elkaar lijken soms toch in verschillende categorieën terechtkomen. Bedrijven hebben bijvoorbeeld veel last van het feit dat de dekzeilen van hun huiftrailers worden opengesneden. In de meeste gevallen gaat het hierbij om pogingen tot ladingdiefstal, maar soms is het evident vandalisme (bijvoorbeeld in gevallen waarin de trailers zichtbaar leeg zijn). Een diefstal met behulp van valse vrachtpapieren is meestal gerangschikt onder verduistering. In gevallen echter waarin geen sprake was van interne betrokkenheid, vallen deze gebeurtenissen bij ons eerder onder oplichting. Daar waar kwesties van deze aard aan de orde zijn, wordt hiervan melding gemaakt bij het bespreken van de onderzoeksbevindingen. De incidenten die in de vragenlijst zijn aangeduid als ‘ongeoorloofde rechtentoekenning’ worden hier niet afzonderlijk besproken. De meeste van deze incidenten betreffen privé-gebruik van bedrijfsmiddelen en zullen aldaar worden besproken.
Ten slotte merken wij nogmaals op dat alleen sprake is van slachtofferschap wanneer incidenten - afzonderlijk of in hun totaliteit- een schade opleveren die bedrijven als problematisch ervaren. Triviale normovertredingen (vanuit de optiek van geleden schade) komen in beginsel derhalve niet voor. Hierbij moet wel worden opgemerkt dat dit een subjectief criterium is; bedrijven kunnen sterk

verschillen in hun beoordeling hiervan. Het ene bedrijf zal bijvoorbeeld het overmatig mee naar huis nemen van pennen wel als schadevol ervaren en het andere niet. Zo gaf één bedrijf aan dat door het afsluiten van de kast met kantoorartikelen, de kosten hiervoor met 30% werden gereduceerd.

3.2 Aard en omvang van gerapporteerde criminaliteit: kwantitatief beeld

Aan bedrijven is de vraag voorgelegd in hoeverre zij -in het algemeen beschouwd- externe en interne criminaliteit beschouwen als een probleem voor hun bedrijf. Tabel 3 bevat de antwoorden op deze vragen. We zien dat bedrijven externe criminaliteit, meer dan interne criminaliteit, beschouwen als een probleem. Voor bijna vier op de tien bedrijven is externe criminaliteit een groot of zeer groot probleem. Voor ruim tweederde van de bedrijven (67%) vormt het tenminste af en toe een probleem. Interne criminaliteit daarentegen wordt door bijna twee op de tien bedrijven als een groot of zeer groot probleem beschouwd. Voor bijna de helft van de bedrijven (48%) is het tenminste af en toe een probleem.

Tabel 3 Externe en interne criminaliteit: waardering van probleem door bedrijven in %

(n=139)	*Externe criminaliteit*	*Interne criminaliteit*
Groot/zeer groot probleem	38%	18%
Enigszins/soms een probleem	29%	30%
Nauwelijks/geen probleem	33%	52%

Aan bedrijven is gevraagd in hoeverre zij in de afgelopen drie jaar slachtoffer zijn geworden van een vijftiental met name genoemde vormen van criminaliteit (zie bijlage 1, blok 4). Daarnaast is gevraagd of deze bedrijven slachtoffer zijn geworden van andere dan de genoemde vormen van criminaliteit. Er is gekozen voor een tijdvak van drie jaar om aldus de minder frequent voorkomende normovertredingen beter te kunnen beschrijven. In tabel 4 worden enkele kengetallen gepresenteerd omtrent slachtofferschap bij de onderzochte bedrijven. Hierbij wordt onderscheid gemaakt naar slachtofferschap in het algemeen (kolom 'Incidenten totaal') en slachtofferschap van interne criminaliteit (kolom 'Incidenten intern').

Tabel 4 Slachtofferschap van bedrijven in afgelopen drie jaar: enkele kengetallen

(n=aantal bedrijven)		*Incidenten totaal*	*Incidenten intern*
Prevalentie van slachtofferschap (alle normovertredingen)		96% (n=139)	87% (n=139)
Aantal *soorten* normovertredingen per bedrijf*			
	Gemiddelde	3,0	2,3
	Mediaan	3	2
	Modus	2	2
		(n=134)	(n=121)
Totaal aantal gerapporteerde incidenten per bedrijf*			
	Gemiddelde	18,0	11,0
	Mediaan	8	4
	Modus	5	1 – 2
		(n=134)	(n=121)

* gebaseerd op selectie van bedrijven die van minimaal één normovertreding slachtoffer zijn geworden. Waarden van uitschieters (bedrijven > honderd gerapporteerde incidenten) naar beneden afgerond op honderd.

We zien in tabel 4 dat bijna alle door ons bezochte bedrijven (96%) in de afgelopen drie jaar slachtoffer zijn geworden van enige vorm van criminaliteit. Een iets kleiner aantal bedrijven, maar nog steeds de overgrote meerderheid (87%), rapporteert in de afgelopen drie jaar slachtoffer te zijn geweest van enige vorm van interne criminaliteit. Veruit de meeste bedrijven die ooit slachtoffer zijn geworden, rapporteren dat ze slachtoffer zijn geworden van verschillende *soorten* normovertredingen. Het gemiddelde aantal verschillende normovertredingen ligt voor alle incidenten op 3,0 (zie tabel). Ruim eenderde van de bedrijven (35%) rapporteert slachtofferschap van vier of meer soorten normovertredingen (niet in tabel). Bij de interne incidenten liggen deze aantallen iets lager: gemiddeld rapporteren bedrijven slachtofferschap van 2,3 soorten interne normovertredingen. Ruim één op de vijf bedrijven (21%) rapporteert slachtofferschap van vier of meer soorten interne normovertredingen (niet in tabel). Hierbij moet worden opgemerkt dat de 'hoog-scorende' bedrijven de gemiddelden iets optrekken (zie waarden mediaan en modus).[16] Ten slotte wordt in tabel 4 ook het totaal aantal gerapporteerde incidenten per bedrijf gepresenteerd: gemiddeld rapporteren bedrijven 22 incidenten over de afgelopen drie jaar, terwijl bij gemiddeld 16 incidenten sprake is van concrete of vermoedelijke interne betrokkenheid. Zoals de waarden van de mediaan en de modus laten zien, worden deze cijfers sterk beïnvloed door de hoog-scorende bedrijven. Als het gaat om slachtofferschap van alle incidenten, is het aantal van 5 het meest gerapporteerd (modus). Bij interne criminaliteit ligt de modus op 1 of 2 incidenten per bedrijf.[17]

Vervolgens zijn we nagegaan van welke vormen van criminaliteit deze bedrijven slachtoffer zijn geworden. De bevindingen hieromtrent worden gepresenteerd in tabel 5. De verschillende vormen van criminaliteit zijn geordend naar prevalentie. De cijfers geven het percentage bedrijven dat in de afgelopen drie jaar éénmaal of vaker slachtoffer is geworden van de genoemde normovertredingen. Ook in deze tabel wordt weer een onderscheid gemaakt naar slachtofferschap in het algemeen (kolom 'Incidenten totaal') en slachtofferschap van interne criminaliteit (kolom 'Incidenten intern').

Tabel 5 Percentage bedrijven dat slachtofferschap rapporteert van afzonderlijke normovertredingen in afgelopen drie jaar (prevalentie in %)

(n=139 bedrijven)	*Slachtoffer van normovertreding (Totaal)*	*Slachtoffer van normovertreding (Intern)*
Inbraak (inclusief auto-/ladingdiefstallen)	77%	34%
Verduistering	66%	61%
Verwijtbaar onprofessioneel handelen	29%	29%
Verbaal of fysiek geweld tegen collega's	17%	17%
Fraude	17%	16%
Oplichting	15%	3%
Overval	14%	5%
Vernieling	14%	8%
Doorspelen bedrijfsinformatie	12%	12%
Illegale handel	11%	3%
Privé-gebruik van bedrijfsmiddelen	11%	11%
Sabotage van werkprocessen	9%	9%
Corruptie	5%	5%

[16] Modus = de score die het vaakst voorkomt. Mediaan = de waarde waaronder en waarboven de helft van de scores valt.
[17] Verdeling is bi-modaal.

Commerciële activiteiten ten eigen bate	3%	3%
Overige	1%	1%

We zien in tabel 5 dat inbraak de meest gerapporteerde vorm van criminaliteit is: ruim driekwart van de bedrijven (77%) is in de afgelopen drie jaar slachtoffer geworden van deze vorm van criminaliteit. Onder inbraak wordt hier dus niet alleen verstaan inbraak in gebouwen, zoals kantoren en loodsen, maar ook diefstallen van en uit (vracht)auto's (cabine- en ladingdiefstallen, diefstallen van complete trailers). Ongeveer eenderde van de bedrijven (34%) rapporteert dat er bij één of meer inbraken concreet of vermoedelijk sprake was van interne betrokkenheid.
Het meest gerapporteerde interne incident betreft verduistering: bijna tweederde van de bedrijven rapporteert slachtofferschap van verduistering in de afgelopen drie jaar. Hierbij gaat het in de meeste gevallen om voorvallen waarbij de dief door uitoefening van zijn werk of anderszins toegang heeft tot de spullen die worden gestolen (verduistering). Dit is de reden dat de percentages voor slachtofferschap totaal en intern (respectievelijk 66 en 61%) zo dicht bij elkaar liggen.
Naast allerhande opzettelijke normovertredingen hebben we bedrijven ook gevraagd in hoeverre zij slachtoffer worden (ofwel schade ondervinden) van personeel dat verwijtbaar onprofessioneel of nalatig handelt. Bijna één op de drie bedrijven (29%) zegt hiermee in de afgelopen drie jaar wel eens te zijn geconfronteerd. Uiteraard gaat het hierbij altijd om interne normovertredingen. Dit geldt ook voor de volgende twee categorieën: verbaal of fysiek geweld tegen collega's en fraude. Één op de zes bedrijven (17%) rapporteert slachtofferschap van deze (bijna altijd interne) vormen van criminaliteit. Bij fraude kan het overigens gaan om zeer uiteenlopende gedragingen, variërend van medewerkers die onterecht een parkeerbonnetje declareren tot en met medewerkers die een bedrijf door hun administratieve manipulaties voor tonnen of zelfs meer benadelen.
Circa één op de zeven bedrijven (14 en 15%) rapporteert slachtofferschap van de normovertredingen oplichting, overval en vernieling. Behalve bij vernieling is volgens de bedrijven slechts in een minderheid van deze gevallen sprake van interne betrokkenheid.
Bijna één op de acht bedrijven (12%) zegt in de afgelopen drie jaar slachtoffer te zijn geworden van (ex-)medewerkers die bedrijfsgevoelige informatie hebben doorgespeeld aan derden (doorgaans concurrenten). Van de bedrijven rapporteert 11% dat medewerkers ongeoorloofd bedrijfsmiddelen voor privé-doeleinden hebben gebruikt. Een zelfde aantal bedrijven (11%) meldt slachtoffer te zijn geworden van personen of organisaties die hun bedrijf hebben gebruikt voor de handel in illegale goederen of diensten (zoals het smokkelen van drugs of mensen via een transport van het bedrijf). In de eerste twee gevallen is altijd sprake van een interne normovertreding. In het derde geval is volgens de respondenten slechts in een zeer beperkt aantal gevallen sprake van interne betrokkenheid. Interne betrokkenheid bij illegale handel is voor bedrijven ook heel moeilijk vast te stellen.
Ten slotte rapporteert een kleiner aantal bedrijven slachtofferschap van uiteenlopende vormen van criminaliteit die altijd een intern karakter hebben: medewerkers die werkprocessen opzettelijk saboteren (9%), medewerkers die steekpenningen aannemen (5%), medewerkers die bedrijfsmiddelen gebruiken voor commerciële activiteiten ten eigen bate (3%) en enkele andere normovertredingen (1%).
In paragraaf 3.4 worden de gerapporteerde incidenten meer in detail besproken.

In tabel 6 is voor de afzonderlijke normovertredingen op een rij gezet met hoeveel incidenten bedrijven in de afgelopen drie jaar te maken hebben gehad (gemiddeld). Deze cijfers zijn gebaseerd op de selectie van bedrijven die slachtoffer zijn geworden van de betreffende normovertreding. Aangezien het hierbij niet altijd om hele grote aantallen gaat, worden de gemiddelden soms sterk beïnvloed door 'hoog-scorende' bedrijven.[18] Ook in deze tabel komt het onderscheid tussen slachtofferschap in het algemeen (kolom 'totaal') en slachtofferschap van interne criminaliteit (kolom 'intern') weer terug.

[18] Het gaat in de meeste gevallen om (rechts)scheve scoreverdelingen. De meeste bedrijven rapporteren 1 of 2 incidenten, maar de kleine(re) groep van bedrijven die 3, 10, 25, 50 of meer incidenten rapporteert, trekt het gemiddelde (soms sterk) omhoog.

Tabel 6 Gemiddeld aantal incidenten in afgelopen drie jaar per onderzocht bedrijf dat slachtoffer is geworden van de betreffende normovertreding

(n=aantal bedrijven)	*Gemiddeld aantal incidenten (totaal) in drie jaar*	*(n)*	*Gemiddeld aantal interne incidenten in drie jaar*	*(n)*
Inbraak (incl. auto-/ladingdiefstallen)	7,2	107	2,3	47
Verduistering	9,4	91	7,9	85
Verwijtbaar onprofessioneel handelen	11,6	40	11,6	40
Verbaal/fysiek geweld tegen collega's	1,6	23	1,6	23
Fraude	4,2	24	4,2	22
Oplichting	2,1	21	1,3	4
Overval	2,8	20	1,4	7
Vernieling	11,9	19	13,0	11
Doorspelen bedrijfsinformatie	1,2	17	1,1	16
Illegale handel	2,9	15	1,5	4
Privé-gebruik van bedrijfsmiddelen	17,5	15	17,5	15
Sabotage van werkprocessen	4,6	12	4,6	12
Corruptie	1,0	7	1,0	7
Commerciële activiteiten ten eigen bate	1,0	4	1,0	4
Overige	1,0	2	1,0	2

We zien bovenaan in tabel 6 bijvoorbeeld dat bedrijven die slachtoffer zijn geworden van inbraak gemiddeld iets meer dan zeven incidenten over de afgelopen drie jaar rapporteren. Gemiddeld rapporteren bedrijven die slachtoffer zijn geworden van inbraken met interne betrokkenheid 2,3 incidenten over de afgelopen drie jaar. Privé-gebruik van bedrijfsmiddelen (17,5 incidenten), vernieling (11,9 incidenten), verwijtbaar onprofessioneel handelen (11,6 incidenten), sabotage van werkprocessen (4,6 incidenten) en fraude (4,2 gevallen van vooral 'kleine fraudes') zijn categorieën die gemiddeld een hogere frequentie halen. Dit ligt voor de hand, omdat dit soort incidenten voor een bedrijf vaak pas een serieus probleem gaat vormen indien ze vaak vóórkomen. Dit geldt in mindere mate ook voor verduistering, waarvan bedrijven gemiddeld 9,4 incidenten rapporteren over de afgelopen drie jaar (7,9 interne incidenten). Van de overige categorieën vallen vooral de relatief hoge frequenties op van illegale handel (gemiddeld 2,9 incidenten per bedrijf in de afgelopen drie jaar, waarvan 1,5 intern) en overvallen (gemiddeld 2,8 incidenten per bedrijf, waarvan 1,4 intern).

3.3 Schade veroorzaakt door (interne) criminaliteit

Op basis van de gegevens die door bedrijven aan ons verstrekt zijn, kunnen we een schatting maken van de schade die bedrijven in deze sector ondervinden van (interne) criminaliteit. Wij presenteren deze schatting met de *nodige slagen om de arm*, omdat het begrip 'schade' nogal problematisch is en omdat verschillende factoren een onbekende invloed uitoefenen op de hoogte van de gerapporteerde schade. De schatting moet daarom vooral worden beschouwd als een *educated guess*. Enkele problemen die een rol spelen bij het schatten van de schade:

- Niet alle schades zijn (goed) in geld uit te drukken (denk aan imagoschade, klantenverlies);
- Schadebedragen kunnen zijn gebaseerd op zeer uiteenlopende 'waarden' (bij verlies van handelsgoederen bijvoorbeeld de productiewaarde, de handelswaarde, de reproductiewaarde, et cetera);
- Als gestolen goederen worden teruggevonden, is niet altijd sprake van (grote) schade;

- Als gestolen goederen zijn verzekerd, bedraagt de financiële schade hooguit het eigen risico of het bedrag boven de verzekerde waarde (wat ook weer sterk kan variëren);
- Respondenten onthouden grote schadebedragen doorgaans beter dan kleine bedragen;
- Respondenten weten in veel gevallen niet wat de schade is, of kunnen deze niet in een bedrag uitdrukken.

Om tot een schatting te komen, gaan we uit van het gemiddelde schadebedrag per gerapporteerd (intern) incident. Dit vermenigvuldigen we met het aantal gerapporteerde (interne) incidenten door bedrijven in de steekproef.[19] Omdat we met name bij grote bedrijven niet altijd over alle vestigingen hebben gesproken, is hiervoor een correctie toegepast.[20] Vervolgens hebben we het verkregen schadebedrag gedeeld door drie, omdat de gerapporteerde incidenten betrekking hebben op een periode van drie jaar en we de schadebedragen per jaar willen weten. De gegevens uit de steekproef zijn daarna geëxtrapoleerd naar de sector (de 285 bedrijven) door het schadebedrag te vermenigvuldigen met de factor 2,04.[21] Omdat het noemen van een specifiek bedrag een onzinnige precisie suggereert, presenteren we de schadebedragen hier in bandbreedtes. Uitgaande van de incidenten en de schades die bedrijven in dit onderzoek aan ons gemeld hebben, komen we tot de volgende schattingen:

- 120 – 160 Miljoen euro per jaar: schade door criminaliteit algemeen (extern én intern)
- 45 – 70 Miljoen euro per jaar: schade door *interne* criminaliteit (onder voorbehoud, waarschijnlijk maakt de schade door *interne* criminaliteit een groter deel uit van de totale schade door criminaliteit, zie verderop in dit hoofdstuk)

Toelichting op de schadebedragen
De schattingen hebben betrekking op bedrijven in de logistieke sector voor wie geldt dat *warehousing* en VAL kernactiviteiten zijn. Via de lijsten van brancheorganisaties hebben we 285 bedrijven gevonden die aan dit criterium voldoen. Het is duidelijk dat deze kleine groep van bedrijven geconfronteerd wordt met een grote schadepost door criminaliteit. Hierbij dienen we wel te bedenken dat veel bedrijven in deze sector grootschalig opereren, vaak vele vestigingen in Nederland hebben en beschikken over een omvangrijk personeelsbestand. De gemiddelde omvang van deze bedrijven ligt ver boven het gemiddelde van het Nederlandse bedrijfsleven.
Verder zijn er tal van factoren die van invloed zijn op de ondervonden schade in deze sector, maar waarvan het effect niet altijd duidelijk is. Als we deze groeperen in factoren die de schade hoger respectievelijk lager kunnen doen uitvallen, dan kunnen we de volgende zaken vermelden:

Factoren die de schadebedragen *hoger* kunnen doen uitvallen:

- De omvang van de populatie van bedrijven die aan onze selectiecriteria voldoet (kernactiviteit: *warehousing* en/of VAL) is niet precies bekend. Er zijn mogelijk nog bedrijven in deze sector waar we geen zicht op hebben.[22] Hiermee is geen rekening gehouden;
- De schadebedragen van sommige incidenten zijn, door een gebrek aan (schade)waarnemingen, niet meegenomen in de schatting. Dit geldt voor: oplichting, het doorspelen van bedrijfsinformatie, illegale handel, privé-gebruik van bedrijfsmiddelen, commerciële activiteiten ten eigen bate, sabotage van werkprocessen, corruptie en geweldsincidenten. Dit zijn overigens niet de belangrijkste incidenten als het om schadeomvang gaat;
- De schades van incidenten waar bedrijven geen zicht op hebben en/of die ze niet aan ons gemeld hebben, zijn niet meegenomen in de schatting.

[19] Voor de invloed van extreem scorende bedrijven is gecorrigeerd door het aantal gerapporteerde incidenten of het schadebedrag per incident te maximeren.
[20] De gerapporteerde incidenten hebben betrekking op 75% van de vestigingen. Om de schade voor de bedrijven in de steekproef in zijn totaliteit te berekenen, hebben we het verkregen schadebedrag derhalve gecorrigeerd met de factor 1,33 (100/75).
[21] Dit is 1 gedeeld door de steekproeffractie (.49).
[22] Dit zijn bedrijven die niet vóórkomen op de door ons gebruikte branchelijsten.

Factoren die de schadebedragen *lager* kunnen doen uitvallen:

- Het aandeel van grote bedrijven in de steekproef ligt waarschijnlijk (dat is niet precies bekend) hoger dan in de populatie. Deze bedrijven rapporteren gemiddeld meer incidenten;
- De geschatte schadebedragen per incident liggen mogelijk hoger dan ze in werkelijkheid zijn, omdat respondenten bij grotere schades vaker kennis hebben van de omvang en vooral deze incidenten met grotere schades aan ons gemeld hebben.

We hebben redenen om aan te nemen dat de schade die bedrijven in deze sector van interne criminaliteit ondervinden, hier te laag geschat is. Bij de conclusie van dit hoofdstuk komen we hierop terug.

Relatieve schade door interne incidenten
Ten slotte hebben we op een rij gezet welke vormen van interne criminaliteit voor de onderzochte bedrijven het meest schadevol zijn, uitgaande van de gemiddelde schade per incident.
Tabel 7 geeft in de tweede kolom een indicatie van het gemiddelde schadebedrag per *intern* incident. Er zijn slechts waarden beschikbaar voor een beperkt aantal normovertredingen. Bij sommige soorten normovertredingen is het niet goed mogelijk om een materiële schade vast te stellen (bijvoorbeeld bij doorspelen van bedrijfsinformatie aan derden), bij andere normovertredingen is het dermate lastig om de materiële schade vast te stellen, dat onze respondenten in veel gevallen geen bedragen paraat hadden. De in tabel 7 genoemde schade-indicaties zijn alleen weergegeven indien tenminste vijf bedrijven schadebedragen hebben genoemd ten gevolge van genoemde interne incidenten.[23]

Tabel 7 Gemiddelde schade-indicaties per *intern* incident bij de onderzochte bedrijven*

(n=aantal bedrijven)	*Gemiddelde schade per intern incident in €*	*Aantal incidenten waarop gemiddelde schade is gebaseerd*
Fraude (n=10)	225.000	38
Overval (n=5)	175.000	7
Inbraak (incl. auto-/ladingdiefstallen) (n=35)	115.000	64
Verwijtbaar onprofessioneel handelen (n=15)	35.000	194
Verduistering (n=53)	15.000	331
Vernieling (n=6)	5.000	119
Privé-gebruik bedrijfsmiddelen (n=5)	4.000	12

* beperkt aantal waarnemingen: alleen berekend indien door tenminste vijf bedrijven schadebedragen zijn genoemd ten gevolge van interne incidenten. De waarden van extreem scorende bedrijven zijn gemaximeerd.

We zien in tabel 7 dat fraudegevallen gemiddeld de grootste schade tot gevolg hebben. Daarna komen de overvallen, gevolgd door de inbraken (inclusief auto-/ladingdiefstallen). Deze drie vormen van interne criminaliteit leiden gemiddeld tot schades die boven de 100.000 euro per incident liggen. Verwijtbaar onprofessioneel handelen kost het bedrijf gemiddeld enkele tienduizenden euro's per incident. Zoals we in paragraaf 3.4 zullen zien, komt deze schade deels voort uit misdrijven (inbraken, ladingdiefstallen) die gepleegd konden worden door nalatigheid van werknemers. De schades bij verduistering, vernieling en ongeoorloofd privé-gebruik van bedrijfsmiddelen liggen doorgaans (veel) lager.
Als we de gegevens in tabel 7 combineren met de gegevens in tabel 6, dan kunnen we vaststellen dat inbraken (inclusief trailer- en ladingdiefstallen) voor deze sector veruit de belangrijkste schadepost

[23] Ter toelichting: de aantallen incidenten waarop de gemiddelde schades per intern incident zijn gebaseerd, vormen een selectie van alle genoemde interne incidenten; alleen interne incidenten waarvan respondenten een schadebedrag konden noemen, zijn in deze tabel vermeld.

vormen: 58% van de ondervonden schade kan aan deze vorm van criminaliteit worden toegeschreven. Als het gaat om schade door interne criminaliteit, dan zijn er uiteenlopende vormen van criminaliteit die hieraan bijdragen.

Hiermee zijn de cijfermatige contouren geschetst van de aard en omvang van de (interne) criminaliteit en de daaruit voortvloeiende schades voor bedrijven in deze sector. In de volgende paragraaf zullen we deze contouren invullen door meer in detail te beschrijven hoe de ervaringen van bedrijven eruit zien en welke kanttekeningen er zijn te maken bij deze bevindingen.

3.4 Ervaringen van bedrijven met interne criminaliteit: het verhaal achter de cijfers

In deze paragraaf gaan we nader in op de cijfers die in de voorgaande paragrafen zijn gepresenteerd. Dit doen we door per normovertreding te beschrijven welke ervaringen bedrijven zoal hebben. Hierbij wordt de volgorde aangehouden van de normovertredingen waarvan de meeste bedrijven last hebben.

3.4.1 Inbraak (inclusief auto-/ladingdiefstallen)

Inbraak is de vorm van criminaliteit waarvan de meeste bedrijven last zeggen te hebben (77%). In totaal zijn in ons onderzoek door 107 getroffen bedrijven 774 inbraken gerapporteerd (over de afgelopen drie jaar). In bijna alle gevallen komen deze incidenten snel aan het licht, omdat er bijvoorbeeld zichtbare braaksporen zijn of er ergens een alarm is afgegaan. Ook het ontbreken van een partij goederen, een vrachtauto of een container wijst het bedrijf snel in de richting van een inbraak. De schade die bedrijven oplopen door deze inbraken varieert sterk: de hoogst gegeven schattingen liggen rond een miljoen euro (per incident), de laagste beginnen bij circa 1.000 euro. Behalve schade door verlies van goederen, wordt hierbij ook vaak braakschade genoemd (deze is met name bij ramkraken vaak aanzienlijk). In enkele gevallen rapporteren bedrijven ook immateriële schade zoals imago- en klantenverlies. Dit laatste doet zich vooral voor wanneer bedrijven herhaald slachtoffer worden. In die gevallen willen de opdrachtgevers/klanten het nog wel eens voor gezien houden. Bedrijven hebben vooral last van *transportgerelateerde inbraken*: diefstal van lading, diefstal van complete trailers en opleggers (meestal met oog op lading), maar ook diefstal van privé-spullen van de chauffeur uit de cabine van de vrachtauto. Uit onze gegevens valt niet af te leiden welk deel hiervan transportgerelateerd is, maar het gaat zeker om meer dan de helft van alle inbraken, mogelijk zelfs 75%. Bij grote ladingdiefstallen, waarbij de complete lading wordt buitgemaakt, wordt vaak de gehele oplegger gestolen. De dieven zorgen dan vaak zelf voor een trekker of stelen deze ter plekke of elders. Nadat de lading is gelost, wordt de oplegger vaak ergens achtergelaten. Volgens gegevens van het LTT wordt dan ook ruim 40% van de gestolen trailers/opleggers weer (meestal leeg) teruggevonden. Volgens onze respondent bij het LTT vinden veruit de meeste lading- en trailerdiefstallen in Nederland plaats in Zuid-Nederland (vooral in Zuid-Oost Brabant en Limburg). Daarnaast blijkt uit de gegevens van het LTT dat in Nederland de meeste trailers worden gestolen vanaf het (eigen) bedrijfsterrein, waar de geladen trailers 's nachts of in het weekend klaar staan voor vertrek.[24] Daarnaast wordt door bedrijven ook vaak melding gemaakt van ladingdiefstal uit vrachtauto's die staan geparkeerd langs de snelweg of op andere onbewaakte plaatsen. Daar bijna alle bedrijven internationaal opereren, beperken deze ladingdiefstallen zich niet tot Nederland; veel ladingdiefstallen vinden juist buiten Nederland plaats. Een veel voorkomende werkwijze bij dit soort inbraken is het opensnijden van de dekzeilen van huiftrailers. Hiervan wordt ook door veel bedrijven in het onderzoek melding gemaakt. Lang niet altijd worden dan ook spullen gestolen. Het lijkt derhalve erop dat de 'dekzeilsnijders' niet in alle gevallen uit zijn op de lading (maar juist op vandalisme) of dat ze willekeurig een aantal dekzeilen opensnijden om aldus te ontdekken waar de interessante lading zich bevindt. In een aantal gevallen melden bedrijven dat ze na het opensnijden van de dekzeilen 'een deel van de lading' missen.

[24] Deze bevinding zien we ook terug in Engels onderzoek waarin naar voren komt dat meer dan de helft van alle gestolen vrachtauto's verdwijnt vanaf het eigen bedrijfsterrein van de getroffen bedrijven (Brown, 1995).

De buit bij ladingdiefstallen bestaat meestal uit goed verhandelbare en waardevolle consumentenartikelen, zoals consumentenelektronica (audioapparatuur, dvd-spelers, pc's en randapparatuur, et cetera), huishoudelijke apparaten, witgoed, persoonlijke-verzorgingsproducten (parfum, scheermesjes en dergelijke), sterke drank, sigaretten, merkkleding enzovoorts. In een klein aantal gevallen gaat het om industriële producten die dan meestal een grote waarde hebben (zoals bijvoorbeeld hoogwaardige metalen en dure machines).
Naast de transportgerelateerde criminaliteit zijn het vooral de inbraken in loodsen en kantoren waarvan bedrijven last ondervinden. Bij de inbraken in loodsen zijn de dieven meestal uit op de daar gestalde handelsgoederen. Hierbij zijn dezelfde goederen in trek als die hiervoor genoemd: de goed verhandelbare en waardevolle consumentenartikelen. Bij de kantoorinbraken zijn het vooral computerschermen (flatscreens), laptops en andere pc-toebehoren waarop de dieven uit zijn. In een kleiner aantal gevallen is men uit op de inhoud van een aanwezige kluis. In een deel van de gevallen bleef de schade voor de bedrijven beperkt, doordat de dieven werden gestoord door de bijna standaard aanwezige detectie- en alarmapparatuur. Dit geldt overigens vooral voor de inbraken in loodsen, die doorgaans beter zijn beveiligd dan kantoren. Echter, ook als er geen spullen worden buitgemaakt, kan het bedrijf nog wel een behoorlijke schade overhouden aan een inbraak.
Digitale inbraken, bijvoorbeeld inbraken in de financiële administratie van een bedrijf of in andere vitale informatiesystemen (om bijvoorbeeld software of gegevens te downloaden), zijn nauwelijks gemeld. Slechts drie bedrijven hebben incidenten van deze aard gerapporteerd.

Interne criminaliteit
Slechts een klein deel van de hiervoor beschreven inbraken (14% ofwel 109 van de 774 incidenten) wordt door de bedrijven gelabeld als intern, dat wil zeggen dat zij bij deze delicten interne betrokkenheid vermoeden. Bij de bedrijven die hiervan melding hebben gemaakt, hebben we gevraagd naar een omschrijving van het laatste incident waarbij sprake is van concrete of vermoedelijke interne betrokkenheid. Als we deze verzameling (van 46 inbraken) bekijken, zien we dat deze afwijkt van het beeld dat hiervoor is geschetst. De 'interne inbraken' zijn vooral inbraken in loodsen (bijna de helft, 48%), inbraken in kantoren (22%) en transportgerelateerde criminaliteit (30%). Bij de laatste categorie moet nog worden opgemerkt dat het in de meeste gevallen gaat om trailer- en ladingdiefstallen die hebben plaatsgevonden op het terrein van het betreffende bedrijf. Verder valt op dat respondenten in veel gevallen de incidenten als intern 'labelen' op grond van vermoedens die zijn gerelateerd aan feiten en omstandigheden rond het incident; in slechts een beperkt aantal gevallen is van deze incidenten een concrete interne verdachte bekend (21%). Meestal komt de identiteit van betrokkene aan het licht doordat het bedrijf zelf onderzoek doet naar de toedracht van de inbraak. Soms schakelt men hierbij ook een particulier recherchebureau in of de politie. Hierop komen wij in hoofdstuk 5 nog uitgebreid terug.
Interne betrokkenheid bij inbraken blijkt vooral uit de volgende zaken: 1) inbrekers hebben gebruik gemaakt van informatie van binnenuit (bijvoorbeeld inbrekers wisten precies hoe ze het alarm moesten uitschakelen, ze wisten meteen de waardevolle goederen te lokaliseren of ze gebruikten voor hun inbraak de enige plek in het bedrijf waar geen alarmsysteem is aangesloten), 2) interne medewerkers hebben de inbraak fysiek gefaciliteerd (dit kan bijvoorbeeld blijken uit alarm dat van een deur is gehaald, een raam dat van binnenuit is opengemaakt, een chauffeur die zijn vrachtauto op een ongebruikelijke plek heeft neergezet zodat deze ongezien kon worden leeggehaald, et cetera) en 3) interne mensen zijn concreet betrokken geweest bij de uitvoering van de normovertreding. In het laatste geval is vaak een concrete interne verdachte bekend. De precieze rol van de interne medewerker kan pas worden bepaald indien het delict volledig is opgehelderd: pas dan kan worden vastgesteld of deze een informerende, faciliterende en/of uitvoerende rol heeft gespeeld. De hiervoor beschreven categorieën van interne betrokkenheid (informatieverschaffing, fysieke facilitering en uitvoering) zeggen derhalve meer over de informatiepositie van het bedrijf dan over de specifieke rol van de interne betrokkenen: hoe meer bedrijven weten van de feiten en omstandigheden rond het misdrijf, hoe beter ze kunnen bepalen of en zo ja, op welke wijze, interne mensen hierbij betrokken zijn.
Uit het voorgaande kunnen we afleiden dat interne betrokkenheid bij inbraken, zoals gerapporteerd door onze respondenten, vooral een functie lijkt te zijn van de kennis die men heeft van de betreffende incidenten. Het zijn vooral incidenten 'dicht bij huis' waarbij men interne betrokkenheid vermoedt.

Dit vermoeden wordt meestal gestaafd door onderzoek ter plekke, waarbij men gebruik kan maken van allerhande beschikbare informatie (zoals camerabeelden, ooggetuigenverslagen, gangbare bedrijfsprocedures, et cetera). De inbraken die onderweg plaatsvinden in vrachtauto's zijn in dit opzicht veel moeilijker te onderzoeken. Het ligt daarom voor de hand om aan te nemen dat de hier gerapporteerde 14% een onderschatting is van het aantal inbraken waarbij sprake is geweest van interne betrokkenheid. Deze conclusie wordt bevestigd door andere bronnen en bevindingen. In paragraaf 3.5.3 gaan we hierop nader in.

3.4.2 Verduistering

Inbraak is, zoals we hiervoor constateerden, de vorm van criminaliteit waarvan de meeste bedrijven slachtoffer worden (hoogste prevalentie). Verduistering daarentegen is de vorm van criminaliteit waarvan bedrijven de meeste incidenten melden (hoogste frequentie): 66% van de bedrijven rapporteert slachtofferschap van verduistering. Dit zijn 91 bedrijven die samen 856 incidenten hebben gemeld. Verduisteringen kunnen op uiteenlopende manieren aan het licht komen: meestal bij de uitvoering van reguliere bedrijfsactiviteiten (er ontbreken bijvoorbeeld goederen die moeten worden verzonden), bij controleactiviteiten (bijvoorbeeld bij een voorraadtelling of bij een visitatie), door melding van een werknemer (die bijvoorbeeld iemand anders iets heeft zien wegnemen), of door melding van een opdrachtgever (die de beloofde goederen niet heeft ontvangen). Af en toe wordt een dief op heterdaad betrapt, zijn er zichtbare diefstalsporen (lege dozen) of komt er een anonieme melding binnen.
Bij het overgrote deel van de gerapporteerde incidenten is volgens de bedrijven sprake van interne betrokkenheid (in 675 van de 856 gevallen, ofwel 79%). In bijna de helft van de interne gevallen (46%) is ook een concrete verdachte bekend. Verdachten komen vooral in beeld naar aanleiding van controle- en onderzoeksactiviteiten door het bedrijf (visitatie, camerabeelden, bedrijfsprocessen onderzoeken, et cetera). In een aantal gevallen worden ze op heterdaad betrapt of meldt een collega de (vermoedelijke) diefstal bij de leiding.
Net als bij inbraken varieert de schade per incident, van nul tot enkele tonnen. Zoals blijkt uit tabel 7 liggen de schadebedragen bij verduistering gemiddeld wel een stuk lager dan bij inbraak. Meestal gaat het hierbij om de waarde van de gestolen goederen. In een enkel geval wordt ook imagoschade genoemd. In een aantal gevallen is de schade voor bedrijven beperkt of nihil, bijvoorbeeld als het verlies van handelsgoederen (als het om deze goederen gaat) binnen een bepaalde contractuele marge blijft, als de gestolen waar later wordt teruggevonden of als de verzekering de geleden schade dekt. Overigens wordt het gemiddelde schadebedrag ook hier beïnvloed door bedrijven die slachtoffer zijn geworden van grootschalige verduisteringen. De meeste verduisteringen die bedrijven rapporteren hebben een vrij laag schadebedrag.
Bij verduistering gaat het in circa tweederde van de gevallen om verduistering van handelswaar uit de loods. In circa één op de zes gevallen gaat het om verduistering van bedrijfsmiddelen. Hierbij gaat het om uiteenlopende zaken als pallets, auto-onderdelen, gereedschap, kantoorspullen, et cetera. In circa één op de tien gevallen gaat het om verduistering van geld (meestal remboursementen, maar ook kas- en kluisgeld). In enkele gevallen is ook verduistering van privé-bezittingen van personeelsleden genoemd (hoewel dit feitelijk buiten het bestek van ons onderzoek valt).[25]
De verduisteringen uit de loods laten zich in twee groepen onderverdelen: kleine en grote verduisteringen. Bij kleine verduisteringen gaat het meestal om individuele producten die uit de loods worden gestolen. Het gaat hierbij meestal om goederen die interessant zijn voor privé-gebruik. Vaak consumentengoederen, levensmiddelen en dergelijke. Verduistering valt vaak niet meteen op, omdat het om individuele producten gaat die bijvoorbeeld uit een doos worden gehaald. De controle van de goederenstroom in een bedrijf kan vaak niet op dit niveau worden georganiseerd, zodat verduistering vaak pas opvalt als de lege dozen aan het einde van een soms lange rit door de logistieke keten aankomen bij de klant. Bij grote verduisteringen komt vaak meer organisatie om de hoek kijken. Dan

[25] Deze categorie -diefstal van privé-bezit van personeel- viel buiten onze bevraging (die gericht was op normovertredingen waar primair het bedrijf zelf slachtoffer van wordt). Het is dus waarschijnlijk dat deze normovertreding veel vaker voorkomt dan nu gemeld door de bedrijven).

gaat het bijvoorbeeld om verduistering van een aantal pallets tegelijk of een complete container die het bedrijfsterrein wordt afgereden. Vaak wordt dit soort verduisteringen uitgevoerd in een situatie waarin sprake is van verminderd toezicht (bijvoorbeeld 's nachts) of in onoverzichtelijke situaties (bijvoorbeeld bij het overslaan van goederen). In het laatste geval belanden de goederen niet geheel per ongeluk in de verkeerde vrachtauto en blijkt de verduistering bijvoorbeeld op het moment dat de 'werkelijke' chauffeur zich meldt om de goederen te laden. De goederen die bij grotere verduisteringen worden buitgemaakt zijn vaak weer goed verhandelbare en waardevolle consumentengoederen en in een enkel geval ook dure industriële producten.
We hebben redenen om aan te nemen dat de gerapporteerde verduisteringen slechts het topje van de ijsberg zijn. Met name waar het gaat om verduistering van handelswaar is het lastig om vast te stellen wat er nu precies allemaal speelt; het ontbreken van goederen kan duiden op vermissing, maar ook op een mistelling of een verkeerde administratieve opgave. Vaak duurt het even voordat duidelijk is wat er nu precies aan de hand is. Als duidelijk is dat er goederen daadwerkelijk zijn vermist, is vaak niet duidelijk waar of wanneer deze vermissing is opgetreden. Daar het logistieke proces soms erg ingewikkeld is (veel overdrachtsmomenten) en er veel verschillende actoren zijn betrokken bij het verwerken van de goederenstroom, kan vaak niet achterhaald worden waar de vermissing precies is opgetreden. Echter, ook als wél duidelijk is dat de goederen in het eigen bedrijf vermist zijn geraakt, leidt dit vaak niet tot de conclusie dat sprake is van verduistering. Veel bedrijven beschouwen een bepaalde mate van breuk of verlies van goederen niet als een problematisch gegeven; immers, waar gehakt wordt vallen spaanders. Vooral als de breuk en het verlies binnen een veilige marge blijven die is afgesproken met de opdrachtgever, is er in beginsel voor het bedrijf geen sprake van een probleem, laat staan een criminaliteitsprobleem. Vaak spreken bedrijven dan ook pas over verduistering als voornoemd breuk-/verliespatroon een voor hen ongewone omvang gaat aannemen of wanneer er een concrete verdachte is. Niet voor niets betreft bijna de helft van alle gerapporteerde verduisteringen een verduistering waarvan een concrete verdachte bekend is. Veel respondenten hebben aangegeven dat hun gerapporteerde verduisteringen alleen de aangetoonde verduisteringen betreffen. Het lijkt ons daarom aannemelijk om te veronderstellen dat de hier genoemde incidenten het topje van de ijsberg vormen.

3.4.3 Verwijtbaar onprofessioneel gedrag

In totaal veertig bedrijven (29% van de steekproef) hebben samen 455 incidenten van verwijtbaar onprofessioneel gedrag gerapporteerd (over de afgelopen drie jaar). In al deze gevallen gaat het om interne incidenten. Het hoge aantal incidenten per bedrijf kan worden verklaard uit het feit dat bedrijven deze incidenten vaak pas als een probleem zien wanneer ze zich veelvuldig voordoen (dit geldt met name voor incidenten waarvan de afzonderlijke schades niet heel hoog zijn). Uit tabel 7 bleek dat de gemiddelde schade per incident niettemin fors is. Dit is voor een belangrijk deel 'bijkomende schade', dat wil zeggen: schade die niet zozeer is voortgevloeid uit het onprofessioneel handelen van de medewerker als zodanig, maar uit de gevolgen van dat handelen. Toelichting: in minstens de helft van de gerapporteerde gevallen gaat het om nalatigheid van met name chauffeurs die hun auto met dure lading onbewaakt hebben achtergelaten of andere (veiligheids)procedures omtrent het vervoer van dure lading niet hebben nageleefd, waarna deze lading kon worden gestolen. Voor het onderhavige onderzoek is dit een interessante bevinding. De gemiddelde schade lag in deze gevallen om en nabij de 100.000 euro (zijnde de gestolen lading). Ook imagoschade en klantverlies werden door bedrijven weer als schadepost genoemd.
De andere helft van de incidenten heeft betrekking op allerhande onnadenkend, onvoorzichtig en roekeloos gedrag binnen het bedrijf. Te denken valt hierbij aan zaken als het stukmaken van rijdend materieel (door onverantwoorde handelingen ermee uit te voeren), het stuk rijden van stellages of laaddeuren in de loods, het verkeerd laden van goederen, het verkeerd plannen van de goederenstroom (waardoor goederen niet, niet goed of niet op tijd aankomen), het verkeerd invullen van formulieren (waardoor vergelijkbare problemen ontstaan), et cetera. Zoals uit één voorbeeld duidelijk naar voren kwam, kan het hierbij soms gaan om 'kleine' fouten met 'grote' gevolgen. In dit voorbeeld had een medewerker bij de verzending een lading grondstoffen omgewisseld, waardoor bij de afnemer de verkeerde grondstoffen in het productieproces terechtkwamen. Gevolg: de complete productie moest worden gestaakt. De afnemer bracht de schade hiervan in rekening bij het bedrijf.

In alle gevallen gaat het om incidenten die zichtbare sporen nalaten, bijvoorbeeld gestolen auto's of lading, maar ook beschadigde bedrijfsmiddelen en dergelijke. In veruit het grootste deel van deze gevallen is ook duidelijk wie binnen het bedrijf hiervoor verantwoordelijk is.

3.4.4 Verbaal of fysiek geweld

Ofschoon deze normovertreding strikt genomen niet binnen onze definitie valt (het gedrag is niet primair gericht tegen het bedrijf), kan het bedrijf hiervan indirect wel veel schade ondervinden, doordat bijvoorbeeld werkprocessen eronder leiden of doordat na verloop van tijd het personeelsverloop toeneemt. Dit staat uiteraard nog los van de emotionele schade die de betrokken werknemers oplopen. Incidenten komen doorgaans aan het licht wanneer de betrokken werknemers of andere collega's hiervan melding maken bij de leiding.
In totaal 23 bedrijven (17% van het totaal) hebben 36 gevallen gemeld, die allemaal een intern karakter hebben. In de meeste gevallen gaat het om min of meer geïsoleerde gevallen. In een enkel bedrijf vormt onderling geweld een meer structureel probleem. Het gaat hierbij vooral om fysiek geweld (mishandeling, vechtpartijen) en bedreiging jegens collega's of superieuren. *Incompatibilité d'humeur* en werkgerelateerde conflicten liggen hier meestal aan ten grondslag. Er zijn daarnaast ook enkele gevallen gemeld van medewerkers die collega's pestten of intimideerden (en ze bijvoorbeeld dwongen om werkprocessen te saboteren). De schade die uit deze incidenten voortvloeit betreft vooral emotionele schade bij de betreffende medewerkers en soms indirecte schade voor het bedrijf (zoals hiervoor beschreven). De genoemde gevallen zijn verder niet specifiek voor de logistieke sector; ze zouden overal kunnen plaatsvinden.

3.4.5 Fraude

Fraude-incidenten kunnen op uiteenlopende manieren aan het licht komen: bijvoorbeeld bij controleactiviteiten (administratieve controles op uitgaven en dergelijke), bij de uitvoering van reguliere bedrijfsactiviteiten (een nieuwe medewerker ontdekt onregelmatigheden van zijn voorganger), en soms ook door melding van een collega of klant. Door 24 bedrijven (17% van het totaal) werden in totaal honderd incidenten genoemd. Bij de meeste bedrijven (16 van de 24) gaat het om allerhande vormen van 'eenvoudige' fraude: teveel uren schrijven, onterecht of teveel onkosten declareren, sjoemelen met vrachtbrieven en dergelijke. Ook het vervalsen van een cv werd genoemd alsmede het gebruik van een valse toegangspas (om vervolgens een verduistering uit te kunnen voeren). Meestal rapporteren bedrijven incidentele gebeurtenissen. In enkele gevallen is bij bedrijven sprake van een situatie waarin deze kleine(re) fraudes zeer regelmatig voorkomen. De afzonderlijke schades zijn vaak niet groot, het is in deze gevallen de hoge frequentie die het probleem vormt. Uiteraard is het de meeste medewerkers te doen om geld of een substituut daarvan, bijvoorbeeld een vergoeding in natura zoals gratis eten, extra vrije tijd, et cetera.
In zes gevallen maakten bedrijven melding van wat we voor het gemak maar even 'witteboordenfraude' zullen noemen. Hierbij gaat het om 'hogere' medewerkers in de organisatie. De uitgebreide(re) bevoegdheden van deze personen en de doorgaans geringe(re) controlemechanismen op dit niveau in de organisatie zorgen ervoor dat de frauduleuze handelingen lang kunnen doorgaan en dat de schades die hierdoor ontstaan doorgaans erg hoog zijn (genoemde schadebedragen liggen tussen honderdduizend en één miljoen euro). De gevolgen kunnen soms zelfs het voortbestaan van het bedrijf bedreigen. Wat verder opvalt aan enkele gevallen is dat met name de managers en directeuren zich niet beperkten tot één soort fraude; er was sprake van een patroon van frauduleuze en andere onrechtmatige en verwijtbare handelingen.
Bijna alle hiervoor genoemde fraudegevallen zijn intern (98 van de 100). Bij deze gevallen is altijd een verdachte bekend. Ontdekking van fraude gaat dus (praktisch) altijd gepaard met ontdekking van de dader(s). Fraude, op enig niveau, kan lang onontdekt blijven, zeker als het gaat om fraudes hoger in de organisatie. Voor 'eenvoudige' fraudes bestaan vaker controleprocedures. De mogelijkheden om op fraude te controleren zijn soms beperkt, bijvoorbeeld omdat de fraude wordt gepleegd door een hoger geplaatste of door iemand die zelf een controlerende functie vervult. Het kan ook om andere redenen moeilijk zijn om fraude te achterhalen. Als voorbeeld een bedrijf waar chauffeurs op verre buitenlanden rijden alwaar zij allerhande contante kosten moeten maken voor bijvoorbeeld eten,

tolwegen, overnachten, et cetera. De redelijkheid van de gemaakte kosten is dan soms moeilijk na te gaan, omdat de landen onbekend zijn en ingediende bonnen zijn opgesteld in een taal die niemand in het bedrijf beheerst. Fraudegevallen komen dan ook vaak bij toeval aan het licht of pas nadat de de gevolgen van de fraude op enigerlei wijze de spuigaten begint uit te lopen en gaat opvallen in de reguliere bedrijfsvoering. Fraude heeft doorgaans ook minder aandacht in het bedrijf dan bijvoorbeeld verduistering van handelsgoederen. Ook kunnen we niet uitsluiten dat respondenten hierover minder gemakkelijk rapporteren dan over andere vormen van interne criminaliteit. We mogen dan ook aannemen dat de gerapporteerde incidenten niet het hele verhaal vertellen.

3.4.6 Oplichting

Door 21 bedrijven (15% van totaal) zijn gevallen genoemd waarin personen of bedrijven onder valse voorwendsels geld, goederen of andere zaken hebben laten leveren. In totaal ging het om 43 incidenten. In de meeste gevallen ging het om personen of bedrijven die (spook)facturen stuurden voor niet geleverde of nooit te leveren diensten (Gouden Gids, internetvermelding, personeelsadvertenties, schoonmaak en dergelijke). Verder noemden respondenten enkele gevallen waarin opdrachtgevers/klanten hun rekeningen niet hadden betaald (niet duidelijk is of het hierbij ook altijd daadwerkelijk om oplichting gaat). Een enkele klant betaalde zijn rekening met een ongedekte cheque.

Interne criminaliteit
De weinige interne gevallen (5 van de 43, ofwel 12%) betroffen twee keer een geval van een 'chauffeur' die met valse vrachtpapieren een lading bij een bedrijf kwam ophalen[26], twee keer een geval van een financieel medewerker die neprekeningen opstelde en aan zichzelf uitbetaalde, en een geval van een zojuist ontslagen medewerker die onder valse voorwendsels erin slaagde een partij goederen mee naar huis te nemen. Deze incidenten zien we in iets andere vorm ook terug bij de gerapporteerde verduisteringen en fraudegevallen. Als we kijken naar het gros van de genoemde incidenten, dan lijkt deze normovertreding vanuit de optiek van interne criminaliteit niet erg relevant: het gaat vooral om externe criminaliteit, die zich ook in andere branches kan voordoen.

3.4.7 Overval

In totaal twintig bedrijven (14% van het totaal) hebben in totaal 46 overvallen gerapporteerd. Op enkele uitzonderingen na ging het hierbij om *transportgerelateerde* criminaliteit, namelijk om overvallen op chauffeurs van vrachtauto's (meestal onderweg). De uitzonderingen betroffen enkele overvallen op een kantoor en op een loods. Bij de overvallen op vrachtauto's is het de overvallers in de meeste gevallen te doen om de (doorgaans dure) lading. In een klein aantal gevallen gaat het om privé-spullen van de chauffeur welke zich in de cabine bevinden (de waarde hiervan is uiteraard gering in verhouding tot voornoemde ladingovervallen). Er wordt door de overvallers gebruik gemaakt van (dreiging met) vuurwapens of er wordt gas in de cabine gespoten om de chauffeur uit te schakelen. De emotionele schade bij de betrokken chauffeurs is evident.

Interne criminaliteit
De als 'intern' gelabelde overvallen (10 van de 46 gevallen ofwel 18%) wijken niet sterk af van de andere overvallen, met uitzondering van het feit dat de meeste van de gerapporteerde kantoor- en loodsovervallen tot deze categorie behoren. Net als bij inbraken zien we hier dus dat bedrijven bij delicten die 'dicht bij huis' plaatsvinden eerder aanwijzingen vinden dat sprake is van interne betrokkenheid. In de helft van de gevallen waarbij sprake is van interne betrokkenheid (vijf van de tien) is een concrete interne verdachte bekend geworden. Politieonderzoek en in één geval een intern onderzoek door het bedrijf brachten deze interne betrokkenheid aan het licht. Interne betrokkenheid kan diverse vormen aannemen: het verlenen van waardevolle informatie aan de overvallers (tip over locatie van aantrekkelijke buit en dergelijke), het creëren van een gelegenheid (hek open zetten, zodat

[26] Deze vorm van oplichting grenst aan sommige diefstalgevallen die we eerder hebben gerapporteerd. In de meeste gevallen zijn deze incidenten als diefstal gekwalificeerd (vanuit het oogpunt van interne betrokkenheid).

overvallers bij het doelwit kunnen komen), of actief meewerken aan het delict (bijvoorbeeld de chauffeur die een overval in scène zet).

3.4.8 Vernieling

Incidenten van vernieling komen bijna altijd aan het licht doordat ze zichtbare sporen nalaten. Door 19 bedrijven (14% van totaal) werden in totaal 226 incidenten gerapporteerd. Bij 143 van deze incidenten is volgens deze bedrijven sprake van interne betrokkenheid (63%). De externe en interne incidenten zijn hier duidelijk te onderscheiden. Het grootste deel van de 'externe' incidenten heeft betrekking op het kapotsnijden van dekzeilen van huiftrailers. Dit komt vaker voor, maar meestal gaat het dan om een (poging tot) ladingdiefstal. Bij de hier gerapporteerde gevallen gaat het om incidenten die louter als vandalisme zijn gelabeld. De overige incidenten betreffen brandstichting, vernieling aan gebouwen en aan bedrijfsmiddelen.

Interne criminaliteit
Bij de interne incidenten gaat het om werknemers die bijvoorbeeld toiletruimtes vernielen, graffiti op deuren spuiten, voertuigen beschadigen, met heftrucks opzettelijk tegen een stellage aanrijden, brandstichting en dergelijke. Opvallend is verder dat een klein aantal bedrijven heel veel van dit soort incidenten meldt. Dit vloeit weer voort uit het feit dat het hier meestal gaat om incidenten met relatief geringe schades, die voor bedrijven pas problematisch worden als ze heel vaak voorkomen. Verder zien we hier een link met de eerder genoemde categorie 'verwijtbaar onprofessioneel gedrag'; het verschil tussen de twee zit hem in het feit dat bedrijven hier opzet in het gedrag waarnemen (het is in een middelgroot bedrijf bijvoorbeeld onwaarschijnlijk dat medewerkers meer dan dertig keer per jaar per ongeluk een wasbak van de muur trekken). Als de opzet niet kan worden aangetoond uit de handeling zelf (bijvoorbeeld een stellage kapot rijden), gaat het doorgaans om gebeurtenissen die door anderen zijn waargenomen en waarbij dus een concrete verdachte in beeld is. Wraak is een motief dat hierbij enkele keren is genoemd.
Het is duidelijk dat bij deze categorie enige onderrapportage mag worden verwacht, omdat bedrijven vaak niet weten of er opzet in het spel is.

3.4.9 Doorspelen bedrijfsinformatie

Deze incidenten komen doorgaans aan het licht doordat bedrijven klanten 'onder verdachte omstandigheden' naar een concurrerend bedrijf zien vertrekken.
In totaal zeventien bedrijven (12%) hebben in totaal twintig incidenten gemeld die allemaal een intern karakter hebben. Meestal gaat het om medewerkers die zijn vertrokken en waardevolle informatie betreffende tarieven, werkwijzen, specifieke offertes en dergelijke hebben meegenomen en doorgespeeld aan hun nieuwe baas. Dit kan door de getroffen bedrijven vaak niet worden hard gemaakt. Niet zelden gebeurt het volgende: bedrijf X ziet een medewerker vertrekken naar bedrijf Y. Snel daarna raakt bedrijf X een belangrijke klant kwijt die vervolgens overstapt naar bedrijf Y. Als de betreffende medewerker ook nog eens met ruzie is vertrokken, is voor de meeste bedrijven wel duidelijk wat er aan de hand is.
Het is niet altijd duidelijk in hoeverre bij deze incidenten sprake is van schending van een concurrentiebeding. De bedrijven hebben daarvan nauwelijks melding gemaakt. Het gaat soms ook om 'grensgevallen': in hoeverre mag een medewerker bijvoorbeeld zijn persoonlijke netwerk gebruiken wanneer hij overstapt naar een ander bedrijf? Het is duidelijk dat het bij deze gevallen altijd gaat om medewerkers met een vitale informatiepositie binnen het bedrijf. De schade die bedrijven hiervan ondervinden -klantverlies, in een enkel geval alleen imagoschade- is moeilijk in geld uit te drukken.

3.4.10 Illegale handel

De smokkel van illegale goederen of diensten komt vaak bij (politie)controles aan het licht. Vijftien bedrijven (11%) hebben in totaal 44 incidenten gerapporteerd. In de meeste gevallen gaat het om het aantreffen van drugs of andere illegale goederen in een lading (zoals heroïne, XTC, illegale sigaretten). Ook noemden respondenten enkele gevallen waarin illegalen op doorreis werden

aangetroffen in een bus of vrachtauto (meestal op weg naar Engeland). Bedrijven kunnen in dat geval hoge boetes krijgen. In twee gevallen ging het om bedrijven waar medewerkers (onderling) drugs verhandelden. De schade die deze incidenten opleveren is voor bedrijven niet altijd even makkelijk in geld uit te drukken. Het kost hen vooral tijd en energie om deze zaken af te handelen. We mogen aannemen dat de gesignaleerde gevallen slechts het topje van de ijsberg laten zien, omdat dit soort incidenten vaak geen sporen achterlaat in het bedrijf. Als deze incidenten onontdekt blijven, ondervinden bedrijven uiteraard ook geen schade ervan.

Interne criminaliteit
Slechts in een gering aantal gevallen was volgens de bedrijven sprake van interne betrokkenheid (in 6 van de 44 gevallen ofwel 14%). In al die gevallen waren er concrete verdachten in beeld (meestal door de politie opgespoord). De interne incidenten wijken niet sterk af van wat we hiervoor hebben beschreven. Het aan het licht komen van deze incidenten hangt sterk af van al dan niet toevallige (politie)controles. In bedrijven waar drugssmokkel een belangrijk probleem is, wordt wel samengewerkt met de politie en worden risicoanalyses uitgevoerd om de kans op betrapping te verhogen.

3.4.11 Privé-gebruik van bedrijfsmiddelen

Ongeoorloofd privé-gebruik van bedrijfsmiddelen wordt door veel bedrijven tot op zekere hoogte toegestaan. De gemelde voorvallen betreffen derhalve incidenten die bedrijven als problematisch ervaren. Ook hier geldt weer dat de lat niet overal op dezelfde hoogte ligt. Sommige bedrijven hanteren een 'nooit'-beleid, anderen zijn erin heel soepel. Vijftien bedrijven hebben in totaal 262 incidenten gerapporteerd. Het gaat in alle gevallen uiteraard om interne incidenten. Deze komen meestal aan het licht door controleactiviteiten die bedrijven uitvoeren. De schades per incident zijn relatief laag (ten opzichte van de andere normovertredingen).
De incidenten betreffen in veruit de meeste gevallen overmatig telefoongebruik voor privé-doeleinden (bijvoorbeeld vaak en lang naar of vanuit het buitenland bellen) en gebruik van tankpassen om privé te tanken. Verder zijn enkele incidenten gemeld die te maken hebben met het ongeoorloofd mee naar huis nemen van vrachtauto's. Een tweetal bedrijven maakte melding van een structureel probleem. Bij veruit de meeste bedrijven betrof het min of meer losse incidenten.

3.4.12 Overige interne normovertredingen

De overige normovertredingen zijn door minder dan één op de tien bedrijven gerapporteerd. We behandelen ze hier in kort bestek. Het gaat in alle gevallen om interne incidenten.

Sabotage van werkprocessen
Een klein aantal bedrijven meldt dat zij wel eens overlast hebben ondervonden van disfunctionerende medewerkers die bijvoorbeeld bewust de planning in de war stuurden (waardoor goederen niet, te laat of verkeerd aankwamen), chauffeurs die weigerden ritten uit te voeren of anderszins het vervoer traineerden, en medewerkers die productieprocessen saboteerden door ergens 'de stekker uit te halen'. Slechts één bedrijf meldde hiervan structureel last te hebben.

Corruptie
Hiervan hebben enkele bedrijven melding gemaakt. In de meeste gevallen ging het hierbij om inkopen of aanbestedingen waarbij de betrokken medewerker een privé-belang had (financieel, maar ook anderszins: de betrokken externe medewerker was bijvoorbeeld een goede vriend van de interne medewerker). Grote corruptiegevallen zijn niet gemeld. Meestal gaat het om kleinere incidenten of om gebeurtenissen waarbij niet goed valt na te gaan of er iets ongeoorloofds aan de hand is. Een voorbeeld van een klein incident: de chauffeur die alleen tankt bij de duurdere tankstations, omdat hij daar airmiles kan krijgen (privé-voordeel). Een voorbeeld van een grensgeval: medewerkers (met name planners of managers) die in de watten worden gelegd (kado's, etentjes) door bedrijven die hierbij een (opdracht)belang hebben. Het is niet altijd duidelijk waar de grens voor bedrijven ligt. We vermoeden

dat dit soort zaken op grote schaal vóórkomt, maar vanwege het 'grenskarakter' vaak niet aan ons gemeld is.

Commerciële activiteiten ten eigen bate
Dit betrof enkele gevallen van chauffeurs die binnen of buiten werktijd hun vrachtauto gebruikten voor ritten waarmee ze (buiten het bedrijf om) extra geld konden verdienen. Deze incidenten kwamen doorgaans aan het licht doordat collega's hiervan melding maakten aan de leiding. In één geval ging het om een manager die onroerend goed dat het bedrijf toebehoorde privé exploiteerde. In dit geval ging het om een incident met een behoorlijke schade voor het bedrijf. In de andere gevallen ging het om kleinere schades.

Overige
Dit betreft slechts twee gevallen. Eén geval betrof een afpersing door een ex-werknemer. Het andere geval betrof een infiltratie in het bedrijf door leden van een criminele organisatie. Deze werd echter ontdekt voordat er misdrijven konden plaatsvinden.

Hiermee besluiten we onze bespreking van de afzonderlijke normovertredingen. In de laatste paragraaf komen we terug op het algemene beeld dat uit deze beschrijvingen naar voren komt.

3.5 Nadere beschouwingen over het *dark number*

Uit het voorgaande is al een enkele keer naar voren gekomen dat het zicht dat bedrijven hebben op het fenomeen 'interne criminaliteit' niet in alle gevallen even volledig is. In deze paragraaf nemen we de *dark number* problematiek nader onder de loep en onderzoeken we in hoeverre en op welke wijze deze de rapportage van normovertredingen ons onderzoek beïnvloedt.

Globaal hebben we de volgende bronnen van onderrapportage kunnen waarnemen:

1 Normovertredingen blijven verborgen (voor anderen in het bedrijf);
2 Gebeurtenissen komen wel aan het licht, maar worden niet als normovertreding gelabeld;
3 Gebeurtenissen worden wel als normovertreding gelabeld, maar niet als een *interne* normovertreding;
4 Respondenten die over normovertredingen rapporteren, hebben een beperkt zicht op wat er gebeurt in het bedrijf;
5 Respondenten die wel zicht hebben op wat er gebeurt in het bedrijf, zijn niet altijd geneigd hierover te rapporteren.

3.5.1 Normovertredingen blijven verborgen

Hierbij gaat het om incidenten waarvan niet-betrokkenen in beginsel niet op de hoogte zijn en die verder ook geen zichtbare sporen achterlaten waaruit anderen in het bedrijf kunnen afleiden dat er iets niet klopt. Bij een overval of een inbraak is meteen duidelijk dat sprake is van een normovertreding. Bij verduistering of opzettelijke beschadiging van goederen is niet altijd duidelijk dat hiervan sprake is, maar vaak laten deze incidenten wel zichtbare sporen na in de zin van vermissingen, manco's en dergelijke. Echter, bij normovertredingen als fraude, corruptie, illegale handel, digitale inbraak, en wellicht ook bij enkele andere normovertredingen, zijn de sporen doorgaans veel minder zichtbaar. Uit voorgaande bespreking blijkt ook dat deze zaken lang verborgen kunnen blijven en vaak bij toeval aan het licht komen.
Het feit dat sommige normovertredingen minder zichtbare sporen nalaten dan andere, is niet alleen een eigenschap van de normovertredingen zelf. Het zegt ook iets over de bedrijfsprocessen die meer of minder (kunnen) worden gecontroleerd. Enkele voorbeelden die we in dit verband zijn tegengekomen en die alle betrekking hebben op de vermissing van goederen:

1 Een bedrijf werkt met levensmiddelen die op gewicht worden verhandeld. Daar bij wegingen afwijkingen kunnen optreden, is het gebruikelijk om gewichtsafwijkingen binnen bepaalde marges te accepteren. Dit schept voor medewerkers een gelegenheid om telkens een klein deel van de lading achterover te drukken zonder dat het bedrijf hierop zicht krijgt;
2 Een bedrijf dat partijen goederen verwerkt zonder te weten welke goederen ze precies verwerken. Dit maakt het lastig om te controleren of er iets ontbreekt;
3 Een bedrijf dat zelf geen systeem heeft om te controleren of goederen ontbreken en afhankelijk is van de klant om te horen of er iets is fout gegaan.

Het is onze ervaring dat bedrijven werkprocessen op lagere niveaus beter in de gaten houden en op dat niveau ook sneller sporen aantreffen die duiden op onregelmatigheden. Dit is bijvoorbeeld het geval bij verduistering van handelsgoederen. Veel bedrijven houden rekening ermee dat dit bij hen gebeurt en treffen maatregelen om deze incidenten zo veel mogelijk te voorkómen of zo goed mogelijk te kunnen traceren. Ten aanzien van allerhande vormen van fraude gebeurt dit veel minder en als het al gebeurt, zijn de maatregelen vaak gericht op het voorkómen van wat we hiervoor 'eenvoudige' fraudes hebben genoemd. Hoe hoger in de organisatie en hoe meer gespecialiseerd de werkzaamheden, des te geringer vaak ook de controlemogelijkheden. Daarnaast hebben we ook gezien dat veel bedrijven criminaliteit impliciet beschouwen als een fenomeen dat gerelateerd is aan de werkvloer. Een sterk veiligheidsbewustzijn ten aanzien van normovertredingen als fraude en dergelijke hebben we praktisch alleen waargenomen bij bedrijven die zelf ooit ervaringen op dit vlak hebben opgedaan.

Samenvattend concluderen we dat incidenten voor bedrijven verborgen kunnen blijven, omdat ze geen zichtbare sporen nalaten in de organisatie. In hoeverre hiervan sprake is, hangt af van het soort normovertreding en van de inspanningen die bedrijven verrichten om deze zaken op het spoor te komen: met name illegale handel, (ingewikkelde) fraude, corruptie en digitale inbraak laten doorgaans minder zichtbare sporen na. Bedrijven hebben vaak ook minder (controle)mogelijkheden om deze incidenten op het spoor te komen.

3.5.2 Gebeurtenissen worden niet als normovertreding gelabeld

Hierbij gaat het om gebeurtenissen die wel worden waargenomen (ze blijven dus niet verborgen zoals hiervoor), maar bedrijven zijn niet in staat óf niet bereid deze gebeurtenissen te labelen als normovertredingen.
Uit het onderzoek komt duidelijk naar voren dat bedrijven op twee fronten problemen hebben om vast te stellen of gebeurtenissen ook normovertredingen zijn. Hierbij gaat het in de eerste plaats om vermissing van (doorgaans handels)goederen. Vermissing van goederen kan uiteenlopende oorzaken hebben: mistelling, verkeerde opgave op de vrachtbrief, de goederen zijn in de verkeerde zending terechtgekomen, et cetera. Vanwege de complexiteit van de logistieke keten kan het soms een tijdje duren voordat de betrokken bedrijven weten dat de betreffende goederen 'terminaal' vermist zijn (dat wil zeggen nergens zijn teruggevonden). Door de vele schakels in de logistieke keten en ook door het feit dat het vaak een tijdje duurt voordat definitief bekend is dat de goederen zijn verdwenen, is het niet altijd mogelijk om na te gaan waar de vermissing is opgetreden. In deze situatie zien we dat bedrijven niet zelden geneigd zijn de problematiek door te schuiven naar de buren in de keten. Echter, ook als duidelijk is dat binnen het bedrijf een vermissing is ontstaan, is niet altijd vast te stellen of sprake is van verduistering. Soms vertelden respondenten ons bijvoorbeeld dat er allerlei geruchten in het bedrijf waren (in verband met verduistering), maar dat ze er niet de vinger achter konden krijgen.
Een tweede categorie die voor bedrijven moeilijk te hanteren is, is het aantonen van *opzet*. Hierbij kan het, net als hiervoor, gaan om vermissing van goederen (verduistering?), maar ook om zaken als beschadiging van bedrijfsmiddelen (opzettelijke vernieling?), fouten in de bedrijfsvoering (sabotage van werkprocessen?), klanten die plotseling weglopen (informatielek?) of nalatigheid van medewerkers (opzet?).
Behalve dat bedrijven niet altijd in staat zijn om vast te stellen of gebeurtenissen duiden op normovertredingen, zijn ze ook niet altijd bereid om dit te doen. Dit uit zich soms in de vorm van naïviteit bij respondenten: niet geloven dat 'dit soort zaken' in het bedrijf vóórkomt. Hier werkt het gezegde 'eerst zien, dan geloven' in omgekeerde richting: 'eerst geloven, dan zien'; bedrijven waar het

veiligheidsbewustzijn laag is, geloven vaak niet dat er onregelmatigheden plaatsvinden en zien deze vervolgens ook niet. Bedrijven die wel geloven in de mogelijkheid van onregelmatigheden, zullen deze ook vaker waarnemen. De bereidheid om gebeurtenissen als normovertredingen te labelen wordt ook beperkt door andere factoren. Een gebeurtenis als normovertreding labelen betekent voor bedrijven dat ze aansprakelijkheid nemen voor die gebeurtenis. Hiervoor spraken we al over het 'doorschuiven van problemen naar de buren in de keten'. Als extern niet kan worden vastgesteld waar een specifiek probleem is opgetreden, en dat komt volgens verzekeraars (en ook volgens andere betrokkenen) heel vaak voor bij vermissing van goederen, zullen bedrijven niet snel geneigd zijn toe te geven dat het probleem bij hen ligt. Bedrijven kunnen zo immers onnodige claims en imagoschade (proberen te) voorkomen.
Ook als een bedrijf geen hinder ondervindt van de gebeurtenissen, zal het niet snel geneigd zijn om deze als normovertredingen te labelen. Zo is het gebruikelijk dat gewerkt wordt met marges waarbinnen manco's in de levering zijn toegestaan. Vermissing of beschadiging van goederen binnen deze marges is voor veel bedrijven daarom geen probleem. Veel bedrijven beschouwen een bepaald percentage (of promillage) manco's als 'standaard'. Ook als de beschadiging of vermissing niet binnen de marges valt, hoeft het voor bedrijven niet altijd een probleem te zijn: soms gaat het om relatief kleine schadebedragen, soms dekt de verzekering de schade. Ook in deze gevallen doen bedrijven vaak niet moeilijk over deze gebeurtenissen (die voor hen dus geen 'problematisch' karakter hebben).

Samenvattend: gebeurtenissen als normovertreding labelen is voor bedrijven niet altijd mogelijk. Daarvoor hebben ze soms een te beperkt zicht. Bovendien hebben ze ook niet altijd belang erbij.

3.5.3 Normovertredingen worden niet als intern *gelabeld*

Hierbij gaat het om gebeurtenissen die door bedrijven wél als normovertreding worden gelabeld, maar waarbij de interne betrokkenheid onduidelijk is. Ook hier kan weer sprake zijn van 'niet-kunnen' en 'niet-willen'.
Bij gebeurtenissen als overvallen, inbraken en soms ook bij vooral grotere verduisteringen, is voor de getroffen bedrijven vaak meteen duidelijk dat sprake is van een normovertreding. Minder gemakkelijk is het voor bedrijven om in deze situaties te achterhalen of er mogelijk sprake is van interne betrokkenheid. Eerder zagen we al dat bedrijven vaker over interne betrokkenheid rapporteren als het gaat om incidenten die dicht bij huis plaatsvinden. Als het gaat om incidenten onderweg, is het voor bedrijven moeilijker om interne betrokkenheid vast te stellen.
Omdat het hier om een categorie gebeurtenissen gaat die voor deze sector erg relevant is, gaan we er hierna wat dieper op in en rapporteren we onze bevindingen uit een aanvullend onderzoek dat we gehouden hebben onder opsporingsdeskundigen op dit terrein.

Een nadere verkenning van interne betrokkenheid bij grote verduisteringen van handelsgoederen (trailer- en ladingdiefstallen, inbraken in loodsen en dergelijke)
Daar (grootschalige) diefstal van handelsgoederen, in welke vorm ook, een aanzienlijk deel uitmaakt van alle gerapporteerde incidenten, hebben we een aanvullend onderzoek uitgevoerd bij opsporingsdeskundigen om na te gaan in hoeverre zij kennis hebben van interne betrokkenheid bij deze vormen van criminaliteit (zie bijlage 3). De deskundigen die wij gesproken hebben zijn het, ieder vanuit hun eigen achtergrond, erover eens dat met name bij grootschalige diefstallen van goederen in de logistieke sector heel vaak (sommige respondenten zeggen: altijd) sprake is van enige vorm van interne betrokkenheid. Deze stelling onderbouwen zij in beginsel op grond van bevindingen uit opsporingsonderzoeken: meestal blijkt bij dit soort delicten dat gebruik is gemaakt van kennis en/of medewerking van binnenuit. In Zuid-Nederland is veel ervaring opgedaan met onderzoeken naar ladingdiefstal. In totaal werden daar door een Boven Regionaal Team vier criminele netwerken opgerold aan wie 150 ladingdiefstallen konden worden gekoppeld. In praktisch alle gevallen gebruikten de dieven kennis die uit de bedrijven zelf kwam. Ook in de Rotterdamse haven wordt de politie regelmatig geconfronteerd met grootschalige diefstallen, van bijvoorbeeld containers, maar ook inbraken in loodsen en dergelijke. De zeehavenpolitie aldaar werkt samen met andere opsporingsorganisaties in het Expertisecentrum Haven dat is gespecialiseerd in de opsporing van strafbare feiten die havengerelateerd zijn en een georganiseerd karakter hebben. Volgens medewerkers

van deze instanties wordt bij grootschalige diefstal bijna altijd gebruik gemaakt van kennis vanuit de organisaties zelf. Ook medewerkers van de Koninklijke Marechaussee op Schiphol bevestigen de bevinding dat met name grootschalige diefstallen (inbraken en dergelijke) moeilijk te plegen zijn zonder informatie van binnenuit. Ten slotte melden ook andere respondenten die we hebben geraadpleegd over deze kwestie, maar wier kennis wellicht iets gefragmenteerder is dan van de voornoemde respondenten, dat bij onderzoek naar dit soort zaken (bijvoorbeeld door expertisebureaus, particuliere recherchebureaus en dergelijke) heel vaak blijkt dat medewerkers uit het bedrijf een rol hebben gespeeld bij de diefstal.
De volgende ervaringen en overwegingen zijn in dit verband aan ons gemeld:

- Veruit de meeste (grootschalige) diefstallen betreffen welgekozen doelwitten, in de meeste gevallen dure en goed verhandelbare consumentengoederen. Het komt maar weinig voor dat spullen worden gestolen die achteraf gezien voor de dieven waardeloos blijken te zijn en die vervolgens dus ook weer ergens worden achtergelaten. De zeehavenpolitie in Rotterdam rapporteerde wel enkele gevallen van ladingdiefstal, waarbij de voor de dieven 'waardeloze' lading achteraf werd teruggevonden. Het betrof hier echter gevallen waarbij de bijbehorende ladingdocumenten de suggestie wekten dat het wél om waardevolle goederen ging. Met andere woorden, het lijkt erop dat de dieven dáárop waren afgegaan. Uit deze bevinding kan worden afgeleid dat de dieven bij grootschalige diefstallen doorgaans op de hoogte zijn van de lading die ze gaan stelen en dat de doelwitten dus niet willekeurig zijn gekozen.
- Om aan de benodigde kennis te komen, kunnen de dieven twee strategieën volgen: ze kunnen via eigen onderzoek en observatie hun doelwitten uitkiezen en/of ze kunnen gebruik maken van kennis van binnenuit. Beide strategieën zien opsporingsdeskundigen voorbijkomen, maar het gebruikmaken van kennis vanuit de organisatie wordt hierbij zo goed als onontbeerlijk geacht. Deze hypothese wordt ondersteund door bevindingen uit opsporingsonderzoeken. Achter de grote diefstallen gaan vaak professionele criminele netwerken schuil. Het stelen, maar vervolgens ook het distribueren en afzetten van grote hoeveelheden goederen vereist een zekere organisatiegraad (zeg maar: een logistieke onderneming). Zonder deze is het niet mogelijk om grootschalige diefstallen uit te voeren. Immers, er zijn vervoermiddelen nodig, los- en laadfaciliteiten, opslagruimte, een geregelde afzetmarkt, voldoende medewerkers, et cetera. Deze organisaties kunnen het zich niet veroorloven om op goed geluk ladingen te stelen. De hoge organisatiegraad vereist een zekere voorspelbaarheid in het proces. Men heeft bijvoorbeeld een afzetmarkt voor bepaalde producten en dus zijn andere producten -hoe waardevol ook- voor deze dieven waardeloos. Kortom, professionals willen van tevoren weten waar ze op af gaan. Alleen kleinere criminelen kunnen het zich 'veroorloven' om bijvoorbeeld willekeurig dekzeilen open te snijden en te kijken of er interessante lading te halen valt. Hierbij gaat het volgens de betrokken opsporingsdeskundigen ook vaker om diefstal van deelladingen (bijvoorbeeld enkele dozen). Kleine criminelen ontberen de faciliteiten die nodig zijn om complete ladingen te kunnen verwerken.
- Observatie alleen levert criminelen doorgaans onvoldoende informatie op over wat ze op enig moment precies kunnen aantreffen in een loods of vrachtwagen. Daarvoor is kennis vanuit de organisatie onontbeerlijk. Bijvoorbeeld: je kunt dagenlang posten bij een bedrijf en erachter komen dat er voortdurend interessante goederen in- en/of uitgaan, maar welke goederen precies wanneer waar zijn, is zonder kennis van de interne processen moeilijk te achterhalen. Hetzelfde geldt voor het leren kennen van beveiligings- en andere organisatieprocedures. Ook hiervoor geldt dat interne kennis nodig is om te weten waar de zwakke schakels in de ketting zich bevinden. Het onderzoek in Brabant heeft laten zien dat één informant (in dit geval een chauffeur) in staat was om in zijn eentje tenminste 120 ladingdiefstallen te faciliteren door de betreffende netwerken van relevante informatie te voorzien (die hij ontlokt had bij collega-chauffeurs).
- Interne betrokkenheid kan zich volgens de opsporingsdeskundigen in zeer uiteenlopende gradaties en in zeer uiteenlopende vormen voordoen. Het kan gaan om medewerkers die relevante informatie doorspelen aan criminelen zonder dit in de gaten te hebben (zie het Brabantse politieonderzoek). Ook het direct benaderen van medewerkers om ze vervolgens om te kopen of onder druk te zetten, is een strategie die wordt gevolgd. Volgens sommige politierespondenten steken criminele netwerken veel tijd en energie in het vinden van geschikte omkoopbare medewerkers. Kwetsbare chauffeurs en in mindere mate planners, loodsbazen en andere functionarissen die kennis

hebben van de goederenstroom zijn hierbij in trek, maar ook hogere functionarissen kunnen deel uitmaken van het (informatie)netwerk van een criminele organisatie. Ook komt het voor dat criminele netwerken proberen om iemand uit hun midden als medewerker in het bedrijf te krijgen.
- Het Brabantse onderzoek naar ladingdiefstallen heeft aangetoond dat een kleine groep daders in staat is om heel veel ladingdiefstallen te plegen en zodoende veel schade te veroorzaken in de sector.

De hier gepresenteerde kennis is gebaseerd op een beperkt aantal onderzoeken, want heel veel ervaring met het uitvoeren van opsporingsonderzoeken naar grootschalige diefstallen in de logistieke sector is er bij de politie niet. De beperking is ook dat bovenstaand verhaal vooral geldigheid heeft voor de diefstallen waarbij grote hoeveelheden goederen worden buitgemaakt. Er zijn volgens de betrokken politierespondenten ook plegers die uit zijn op snel succes en die *hit-and-run* delicten plegen. Zij snijden bijvoorbeeld dekzeilen open en kijken of er wat te halen valt. Hierbij speelt het gelegenheidselement een grotere rol.
Voor ons is van belang te constateren dat bedrijven in deze sector een groot probleem ervaren waar het gaat om grootschalige diefstal van handelsgoederen. Ze zien dit vooral als een extern probleem. Slechts in een gering aantal gevallen weten of vermoeden ze dat sprake is van interne betrokkenheid (bijvoorbeeld bij 14% van de inbraken en bij 18% van de overvallen). Een rondgang langs enkele opsporingsinstanties laat echter een volstrekt ander beeld zien: bij de opgehelderde zaken is in de meeste gevallen juist wel sprake van interne betrokkenheid (in enige vorm). Op grond van deze gegevens concluderen we dat bij de inbraken, en mogelijk ook bij enkele andere normovertredingen, zoals overvallen en grootschalige diefstal, veel vaker dan nu wordt gedacht of aan ons gemeld, sprake is van interne betrokkenheid in enige vorm.
[Einde nadere verkenning]

Naast het feit dat bedrijven moeite hebben om interne betrokkenheid vast te stellen, zien we ook hier weer dat bedrijven soms niet bereid zijn om aan te nemen dat interne mensen betrokken zijn bij normovertredingen. Een psychologisch mechanisme dat hierbij een rol speelt is dat sommige respondenten gebeurtenissen buiten de muren van het bedrijf automatisch als iets externs definiëren, terwijl gebeurtenissen binnen de muren eerder als intern worden gedefinieerd. Ook hier spelen naïviteit, gebrek aan ervaring en dergelijke, een rol als het gaat om het niet willen zien van deze mogelijkheid. Echter, ook sociale omstandigheden in het bedrijf kunnen hierbij een rol spelen. Met name in kleinere bedrijven en in familiebedrijven vindt men het doorgaans heel lastig om te overwegen dat collega's betrokken zijn bij zaken die niet door de beugel kunnen. De directeur kent zijn personeel vaak al lang (en vaak ook persoonlijk) en de verhoudingen in het bedrijf zijn informeel en gebaseerd op onderling vertrouwen. Voorbeeld: in een klein bedrijf worden persoonlijke bezittingen gestolen van medewerkers. Op de vraag van de interviewer of hierbij mogelijk interne mensen betrokken zijn, antwoordt de respondent dat hij vermoedt dat externe chauffeurs de dieven zijn. Waarom externe chauffeurs? Omdat deze toegang hebben tot de betreffende ruimte. De personeelsleden zelf hebben uiteraard ook toegang. Toch lijkt het de respondent onwaarschijnlijk dat die voor de diefstallen verantwoordelijk zijn (ter toelichting: het bedrijf wordt per dag door hooguit enkele chauffeurs bezocht, terwijl de betreffende ruimte dagelijks door tientallen medewerkers wordt gebruikt die meermalen per dag gebruik ervan maken). In hoofdstuk 5 zullen we zien dat dit soort bedrijven na ervaringen met criminaliteit soms veel moeite hebben om controlemaatregelen zoals camera's en dergelijke in te voeren. Het personeel ervaart deze maatregelen als een inbreuk op een verworven vertrouwenspositie.

Samenvattend kunnen we concluderen dat bedrijven niet altijd zicht hebben op interne betrokkenheid bij normovertredingen. Als het gaat om grootschalige diefstallen van handelsgoederen hebben we aannemelijk gemaakt dat hierbij veel vaker dan bedrijven denken (of aan ons rapporteren) sprake is van interne betrokkenheid. Daarnaast willen bedrijven de interne betrokkenheid niet altijd zien. Psychologische en sociale mechanismen zorgen voor onderrapportage bij met name kleinere en informelere organisaties.

3.5.4 Respondenten hebben een beperkt zicht op wat er in het bedrijf gebeurt

Normovertredingen kunnen plaatsvinden en ook bekend zijn in een bedrijf, maar niet bij de persoon die hierover aan de onderzoekers rapporteert. Deze onderrapportagebron is deels een gevolg van de gebruikte onderzoeksopzet om per bedrijf één persoon te interviewen. Met name in grotere bedrijven met meer vestigingen is onderrapportage opgetreden doordat de kennispositie van de respondent soms niet verder reikte dan de eigen vestiging of enkele van de vele vestigingen die bedrijven soms rijk zijn. In een enkel geval bleek de best geïnformeerde persoon binnen het bedrijf toch nog heel weinig te weten van wat er allemaal omging buiten zijn directe gezichtsveld. Normovertredingen die bijvoorbeeld op de werkvloer bekend zijn, of bij een andere afdeling, hoeven ook niet altijd het management, in casu onze respondent, te hebben bereikt. Ook respondenten die nog niet zo lang voor het bedrijf werken of pas sinds kort hun huidige functie bekleden, zijn niet altijd optimaal geïnformeerd. Daarnaast speelt ook de eigen focus van de respondent een rol. In sommige bedrijven zijn respondenten heel breed georiënteerd op allerhande mogelijke normovertredingen, in de meeste bedrijven echter focussen de respondenten zich op een beperkt aantal verschijnselen, bijvoorbeeld de verduistering van handelsgoederen.

Samenvattend: er kunnen verschillende oorzaken ten grondslag liggen aan het feit dat respondenten niet alle normovertredingen in hun bedrijf kunnen overzien.

3.5.5 Respondenten willen niet over normovertredingen rapporteren

Hierbij gaat het om gevallen waarin de respondent weliswaar op de hoogte is van de normovertredingen in het bedrijf, maar ervoor kiest hierover niet te rapporteren aan de onderzoekers. Uiteraard gaat het hierbij om een subjectieve beoordeling door de interviewers, gebaseerd op de antwoorden en de waargenomen houding van de betrokken respondenten. Bij circa 20 van de 139 interviews (15%) hebben de interviewers aangegeven dat ze het vermoeden hadden dat de respondent niet het achterste van zijn of haar tong liet zien of een te rooskleurig beeld schetste van de situatie in het bedrijf (dit kan ook betrekking hebben op de beveiligingssituatie). Soms had dit te maken met de respondent zelf, bijvoorbeeld een gesloten type, of iemand die het eigen functioneren in een gunstig kader wilde plaatsen door bij de beveiligingsmaatregelen te overrapporteren (‘alles is hier op orde’) en bij de incidenten te onderrapporteren (‘er kan hier weinig gebeuren’). Vaker echter leek de terughoudendheid voort te komen uit de behoefte om het bedrijf niet in een ongunstig daglicht te plaatsen (wellicht uit angst dat de verstrekte informatie mogelijk toch ergens zou kunnen uitlekken). Echter, ook overwegingen die hiervoor al aan de orde zijn geweest kunnen hierbij een rol spelen. Zo kan de respondent bijvoorbeeld weten dat er een vermissing van goederen in zijn bedrijf is opgetreden (die hij ook labelt als een interne verduistering), maar hij zal met de onderzoekers moeilijk erover kunnen praten als hij tegenover de verzekeringsmaatschappij heeft volgehouden dat de vermissing niet in zijn bedrijf is opgetreden.
Verschillende respondenten hebben voorafgaand aan en ook tijdens de interviews geïnformeerd naar de vertrouwelijkheid waarmee de verstrekte informatie zou worden behandeld. Een enkele respondent wilde deze toezegging zwart op wit vastgelegd zien. Een en ander maakt duidelijk hoezeer bedrijven met name bevreesd zijn voor imagoschade als bekend wordt met welke problemen ze kampen. Onze indruk is dat deze bron van onderrapportage vooral de *interne* criminaliteit betreft en in (veel) mindere mate de externe criminaliteit. Overigens moet hier worden opgemerkt dat deze bron van onderrapportage tijdens het veldwerk veel geringer leek dan we vooraf hadden gedacht. We waren vaak verbaasd over de openheid van respondenten en het gemak waarmee ze allerhande criminaliteitsproblemen met ons wilden delen. We geloven dan ook dat deze bron van onderrapportage er één is in de rij (zie hiervoor) en niet dé bron van onderrapportage (zoals vaak wordt gedacht bij dit soort onderzoek). Het is duidelijk dat er bij bedrijven een spanningsveld bestaat tussen het praten over en openbaar maken van criminaliteitsproblemen enerzijds en het effectief bestrijden van deze problemen anderzijds. Wij denken dat een klein aantal bedrijven (de vermoedelijke 15%) de ‘veilige’ anonieme setting van het onderzoek nog te onveilig vond om over deze problemen vrijuit te praten.

Samenvattend: respondenten in bedrijven zijn soms terughoudend in het rapporteren van met name interne incidenten. Bedrijfsbelangen en soms ook persoonlijke belangen liggen hieraan ten grondslag.

In tegenstelling tot wat de term *dark number* doet vermoeden, gaat het hierbij per definitie niet om een kwantitatief te bepalen verschijnsel. Wij kunnen niet aangeven hoeveel interne normovertredingen niet gerapporteerd zijn (die wel hebben plaatsgevonden). Wat we wel kunnen, is aangeven waar onderrapportage aannemelijk is en op welke gronden. In deze paragraaf hebben we laten zien dat onderrapportage zeer uiteenlopende achtergronden kan hebben en dat deze achtergronden bij verschillende bedrijven en bij verschillende soorten normovertredingen kunnen leiden tot onderrapportage. In weinig bedrijven zullen de hiervoor genoemde onderrapportagebronnen allemaal even prominent aanwezig zijn. Het overzicht laat echter wel zien dat onderrapportage een zeer significant verschijnsel is waarmee we rekening moeten houden bij het duiden van de bevindingen (zie hierna paragraaf 3.7).

3.6 Bevindingen in het licht van eerder onderzoek

Onderzoekers van het *Australian Institute of Criminology* hebben een groot aantal studies uit verschillende landen vergeleken waarin slachtofferschap van bedrijven van criminaliteit is onderzocht (AIC, 2004). Zij concluderen dat twee bevindingen zo'n beetje 'standaard' zijn: 1) overal lopen bedrijven een hoog risico om slachtoffer te worden van criminaliteit. Het risico ligt voor bedrijven doorgaans aanzienlijk hoger dan voor individuen en huishoudens, en 2) veel van deze criminaliteit is geconcentreerd in een beperkt aantal sectoren van de economie, waarbij winkel-, horeca- en productiebedrijven er vaak uit springen als het gaat om gerapporteerde incidenten (TrendMeter, 2000; NIPO, 2002; AIC, 2004).
Als we de gegevens uit ons onderzoek vergelijken met gegevens uit vergelijkbare studies, kunnen we constateren dat het criminaliteitsprobleem in de door ons onderzochte sector qua omvang ruim boven het gemiddelde van het bedrijfsleven in Nederland ligt. In de Monitor Bedrijven en Instellingen (NIPO, 2002) geeft eenderde van de bedrijven aan criminaliteit te beschouwen als een probleem waar ze enigszins of serieus last van hebben. In onze steekproef ligt dit aantal twee keer zo hoog (op tweederde). Ook ten aanzien van interne criminaliteit zijn de verschillen tussen deze en andere studies groot te noemen. In een onderzoek van PriceWaterhouseCoopers uit 2003 geeft 38% van de deelnemende bedrijven (uit verschillende sectoren) aan in de afgelopen twee jaar getroffen te zijn door interne fraude en diefstal (PWC, 2003). In een onderzoek van VNO-NCW uit 2003, ook onder bedrijven uit verschillende sectoren, geeft 36% van de bedrijven aan in de afgelopen drie jaar slachtoffer geworden te zijn van criminaliteit door eigen medewerkers. In een onderzoek van de stichting TrendMeter (ook bij bedrijven uit verschillende sectoren) ligt het aantal bedrijven dat zegt in de afgelopen drie jaar slachtoffer geworden te zijn van interne criminaliteit, even boven de 50% (TrendMeter, 2000). Ter vergelijking: in ons onderzoek ligt het percentage bedrijven dat zegt slachtoffer geworden te zijn van enige vorm van interne criminaliteit in de afgelopen drie jaar op 87%. Uiteraard moeten we bij het vergelijken van dit soort cijfers rekening houden met verschillen in de gevolgde onderzoeksmethodologie, maar de uitkomsten van de verschillende vergelijkingen wijzen telkens in dezelfde richting, namelijk dat de omvang van de problematiek in de door ons onderzochte sector aanzienlijk groter is dan gemiddeld in het Nederlandse bedrijfsleven.
Als we kijken naar het soort incidenten waar bedrijven slachtoffer van worden, dan laat deze studie vooral overeenkomsten zien met andere studies. Het zijn vooral vermogensdelicten en in het bijzonder verduisteringen van (handels)goederen waar bedrijven de meeste last van zeggen te hebben (Cools, 1994; TrendMeter, 2000; NIPO, 2002; VNO-NCW, 2003; AIC, 2004). Echter, ook vernieling komt in sommige studies prominent naar voren, zoals onder andere blijkt uit een studie van de Britse Kamers van Koophandel (BCC, 2004), maar ook uit de Monitor Bedrijven en instellingen (NIPO, 2002) en uit het overzicht van het *Australian Institute of Criminology* (AIC, 2004).
Ook ten aanzien van vormen van (interne) criminaliteit die bedrijven in veel mindere mate melden, vertoont deze studie sterke overeenkomsten met andere onderzoeken. Zo constateert Cools (1999) dat bedrijven nauwelijks melding maken van bijvoorbeeld computercriminaliteit. Het is hem niet duidelijk of de oorzaak hiervan moet worden gezocht in het feit dat deze incidenten minder frequent vóórkomen of dat ze zich moeilijker laten opsporen. Green rapporteert in dit verband een schatting van het Amerikaanse leger; deze organisatie gaat ervan uit dat de kans op ontdekking van computercriminaliteit niet hoger is dan circa 1% (Green, 1990). Ook gedrag dat Hollinger en Clark

(1982) aanduiden als *production deviance* (hier aangeduid als: sabotage van bedrijfsprocessen) is in dit onderzoek nauwelijks door bedrijven gemeld. Uit de studie van Hollinger en Clark (onder werknemers zelf!) blijkt dat tenminste driekwart van het personeel zich hieraan met enige regelmaat schuldig maakt. Wij vermoeden dat dit voor veel bedrijven, zeker vanuit de optiek van geleden schade, een te vaag en onzichtbaar probleem is.
Ten aanzien van de betrokkenheid van interne medewerkers bij met name grootschalige diefstal van handelsgoederen vinden we ook in andere studies aanwijzingen dat hiervan veel vaker sprake is dan de bedrijven in dit onderzoek (ons willen doen) geloven (Fijnaut et al., 1995). Van Dijk et al. (1999) constateren dat bij grootschalige vermogenscriminaliteit in de Rotterdamse haven vaak sprake is van betrokkenheid van personeel, dat hierbij hand- en spandiensten verricht voor buitenstaanders. Ook in Engelse, Amerikaanse en Australische studies wordt hiervan melding gemaakt (McKinnon en Heinrich-Jones, 2000; Mayhew, 2001). Atkinson (2001) beweert dat bij 80 tot 99% van alle grootschalige ladingdiefstallen in de Verenigde Staten sprake is van enigerlei interne betrokkenheid.

Samenvattend kunnen we stellen dat de door ons onderzochte sector gemiddeld meer last ondervindt van (interne) criminaliteitsproblemen dan andere sectoren in de Nederlandse economie. De aard van de problematiek wijkt echter niet sterk af van die in de andere sectoren: het zijn vooral vermogensdelicten, in het bijzonder diefstal van handelsgoederen, waar bedrijven veel last van hebben. De bevinding dat bij grootschalige diefstal van handelsgoederen vaak sprake is van interne betrokkenheid, zien we ook terug in ander onderzoek.

3.7 Samenvatting en conclusie

Omvang van het criminaliteitsprobleem
Voor een royale meerderheid van de bedrijven is criminaliteit een probleem waarmee zij soms of vaker te maken hebben. Bijna één op de vier bedrijven noemt criminaliteit zelfs een groot of zeer groot probleem. Interne criminaliteit wordt door deze bedrijven minder vaak als een probleem gezien. Toch noemt bijna de helft van de bedrijven dit als een probleem waarmee ze soms of vaker te maken hebben. Voor minder dan één op de vijf bedrijven is interne criminaliteit een groot of zeer groot probleem. Bijna alle bedrijven zijn in de afgelopen drie jaar slachtoffer geworden van enige vorm van criminaliteit (of andersoortige normovertredingen). De meeste bedrijven werden meermalen slachtoffer van uiteenlopende vormen van criminaliteit. Als het om interne criminaliteit gaat liggen de cijfers iets lager, maar ook hiervoor geldt dat de overgrote meerderheid van de bedrijven er in de afgelopen drie jaar mee te maken had, meestal (veel) vaker dan eens. Als we deze bevindingen afzetten tegen bevindingen uit eerder onderzoek, moeten we concluderen dat de door ons onderzochte sector bovengemiddeld wordt getroffen door (interne) criminaliteit. Hierbij moeten we overigens niet uit het oog verliezen dat het onderzoek heeft plaatsgevonden bij bedrijven van zeer verschillende omvang (zie hoofdstuk 2). De genoemde cijfers worden uiteraard beïnvloed door het feit dat (zeer) grote ondernemingen een significant deel van de steekproef uitmaken.
Het onderscheid tussen interne en overige (externe) criminaliteit is soms moeilijk te maken. Dit heeft enerzijds te maken met een gebrek aan kennis: het is niet altijd bekend of een normovertreding een intern karakter heeft. In zo'n geval is voor de betrokken bedrijven sprake van een *externe* normovertreding. Anderzijds zorgen psychologische en sociale mechanismen soms ervoor dat bedrijven de mogelijkheid van interne betrokkenheid bij normovertredingen liever niet onder ogen willen zien.

Aard van de gerapporteerde (interne) criminaliteit
Diefstal van handelsgoederen en dan met name grootschalige diefstal in de vorm van trailer- en ladingdiefstallen, inbraken in loodsen, overvallen op vrachtauto's en andere grootschalige verduisteringen uit loodsen of vanaf bedrijfsterreinen vormen voor deze sector veruit het belangrijkste criminaliteitsprobleem. Meestal gaat het om diefstal van waardevolle en goed verhandelbare consumentengoederen zoals consumentenelektronica, pc's en toebehoren, witgoed, merkkleding, persoonlijke verzorgingsproducten, et cetera. In heel veel gevallen gaat het om incidenten die op de een of andere wijze zijn gerelateerd aan de transportfunctie. Ter nuancering moet hieraan worden

toegevoegd dat bijvoorbeeld de diefstal van een (geladen) trailer weliswaar transportgerelateerd is, maar dat uit de opgave van het KLPD/LTT blijkt dat veruit de meeste trailers worden gestolen vanaf de eigen bedrijfsterreinen van de betreffende bedrijven. Transport betekent dus niet altijd 'onderweg'. Volgens de bedrijven is bij deze incidenten slechts in een gering aantal gevallen sprake van interne betrokkenheid. Een nader onderzoek onder opsporingsdeskundigen laat echter zien dat zij juist in de meeste gevallen enige vorm van interne betrokkenheid waarnemen (gebaseerd op zaken die zij ophelderen). Deze bevinding brengt ons ertoe te concluderen dat bij deze delicten veel vaker dan bedrijven denken of aan ons rapporteren, sprake zal zijn van interne betrokkenheid. Deze kan, zoals we hebben gezien, uiteenlopende vormen aannemen: onbewust of bewust informatie lekken, het misdrijf fysiek faciliteren of zelf meewerken aan de uitvoering.
Verduistering van handelsgoederen uit de loods wordt ook door veel bedrijven gemeld als een criminaliteitsprobleem. Hierbij gaat het veel vaker om kleinere verduisteringen door medewerkers van het bedrijf. In tegenstelling tot de diefstallen die hiervoor aan de orde waren, gaat het hierbij niet om complete ladingen, maar om verduistering van bijvoorbeeld een doos of enkele dozen of van producten uit dozen. Vaak definieert een bedrijf een vermissing van goederen pas als een verduistering als ze een concrete verdachte op het oog hebben, meestal een medewerker in de loods die door zijn werk toegang heeft tot de begeerde goederen. In veel gevallen beschouwen bedrijven de vermissing of beschadiging van kleine hoeveelheden handelsgoederen echter niet als een (criminaliteits)probleem.
Verder noemen bedrijven uiteenlopende interne problemen. Bedrijven die te maken hebben gehad met een inbraak of een ladingdiefstal melden nogal eens dat medewerkers in die gevallen nalatig zijn geweest door een hek open te laten staan of door hun auto onbeheerd achter te laten, et cetera. Ook onderling geweld wordt door een aantal bedrijven genoemd als een probleem dat wel eens aan de orde is. Een deel meldt ook fraudegevallen. In de meeste gevallen gaat het hierbij om 'eenvoudige' fraudes zoals onterechte opgaven bij kostendeclaraties en dergelijke. Uit de gerapporteerde gevallen van 'witteboordenfraude' komt naar voren dat deze zaken lang verborgen kunnen blijven in een bedrijf. Het valt dan ook niet uit te sluiten dat als het om dit soort fraudes gaat, sprake is van onderrapportage in het onderzoek. Dit geldt ook voor corruptie en betrokkenheid bij handel in illegale goederen.
Sommige bedrijven meldden incidenten als opzettelijke vernieling van bedrijfsmiddelen, sabotage van werkprocessen en dergelijke. Ook hierbij is waarschijnlijk sprake van onderrapportage, omdat bedrijven heel moeilijk kunnen vaststellen of sprake is geweest van opzettelijk gedrag. Een aantal bedrijven meldt last te hebben gehad van vertrekkende medewerkers die bedrijfsgevoelige informatie hebben meegenomen en doorgespeeld aan een concurrent. Meestal kunnen ze dit feit niet hard maken, maar bestaat er een sterk vermoeden op grond van feiten en omstandigheden.

Dark number ten aanzien van interne criminaliteit
Uit voorgaande bespreking wordt duidelijk dat het moeilijk is om harde grenzen te trekken rond het verschijnsel interne criminaliteit. Daarvoor is het probleem van de onderrapportage te prominent. Dit doet zich bij allerlei incidenten in verschillende vormen voor. Sommige incidenten kunnen goed verborgen blijven, zoals fraude, corruptie of digitale inbraak. Bij andere incidenten zijn bedrijven soms niet in staat of niet bereid om te bepalen of het om normovertredingen of iets anders gaat, zoals bij vermissing van goederen (verduistering?), beschadiging van goederen of bedrijfsmiddelen (opzettelijke vernieling?), fouten in het productieproces (sabotage?). Bij weer andere normovertredingen zijn bedrijven niet in staat of bereid om vast te stellen dat sprake is van interne betrokkenheid, zoals bij overvallen, inbraken, verduisteringen en illegale handel. Het vermogen en de wil van bedrijven om incidenten te ontdekken, om ze als zodanig te labelen en om erachter te komen dat sprake is van interne betrokkenheid, varieert uiteraard ook. In sommige bedrijven worden bedrijfsprocessen in het algemeen en onregelmatigheden in het bijzonder aanzienlijk beter in de gaten gehouden dan in andere bedrijven. Deze bedrijven 'zien' vaak meer (interne) incidenten.
Respondenten in ons onderzoek zijn ook niet altijd volledig geïnformeerd en als dat wel het geval is, zijn ze niet altijd bereid om hun ervaringen (volledig) te delen met de onderzoekers. Kortom, we mogen aannemen dat het door de bedrijven gepresenteerde beeld niet het volledige beeld is.
Echter, op grond van de bevindingen zoals deze nu voorliggen, rekening houdend met de kanttekeningen die we hierbij hebben geplaatst, concluderen we dat de sector waarin wij onderzoek hebben gedaan, te maken heeft met een serieus criminaliteitsprobleem, zowel naar aard als naar

omvang. Het ‘interne’ karakter van dit probleem is, zoals wij aannemelijk hebben gemaakt, waarschijnlijk veel groter dan veel bedrijven in deze sector veronderstellen.

Ondervonden schade
Op basis van gegevens omtrent incidenten en schades die bedrijven in dit onderzoek aan ons hebben gemeld, komen we tot de conclusie dat de schade die deze sector ondervindt van criminaliteit in het algemeen en van interne criminaliteit in het bijzonder, groot te noemen is. De schade door criminaliteit in het algemeen (intern én extern) bedraagt naar schatting jaarlijks 120 tot 160 miljoen euro. De schade door interne criminaliteit is geschat op 45 tot 70 miljoen euro. Als we rekening houden met de bevinding dat met name bij grootschalige diefstallen van handelsgoederen heel vaak interne medewerkers betrokken zijn, moeten we concluderen dat de genoemde schade door *interne* criminaliteit waarschijnlijk een royale onderschatting betreft van de werkelijk geleden schade.

4 Kenmerken van slachtoffers en daders van interne criminaliteit

In dit hoofdstuk beschrijven we onze bevindingen ten aanzien van de onderzoeksvragen 2 en 4.

- *Wat zijn de kenmerken van bedrijven die in meer of mindere mate met verschillende vormen van interne criminaliteit worden geconfronteerd?*
- *Welke relevante kenmerken hebben de bekende daders van de verschillende vormen van interne criminaliteit?*

In paragraaf 4.1 gaan we in op de vraag welke bedrijven meer dan andere slachtoffer worden van (verschillende vormen van interne) criminaliteit. In paragraaf 4.2 bespreken we de kenmerken van daders van interne criminaliteit, voorzover deze bekend zijn bij de bedrijven die we hierover hebben bevraagd. In paragraaf 4.3 maken we, ten aanzien van onze bevindingen over de daders, een vergelijking met eerder onderzoek. In paragraaf 4.4 brengen we deze bevindingen bij elkaar en doen we samenvattende uitspraken over de factoren die ten grondslag liggen aan interne criminaliteit in bedrijven.

4.1 Bedrijfskenmerken die samenhangen met slachtofferschap van interne criminaliteit

In tabel 8 is een aantal bedrijfskenmerken afgezet tegen het gemiddelde aantal incidenten dat deze bedrijven hebben gemeld over de afgelopen drie jaar.[27] Hierbij is wederom een onderscheid gemaakt tussen interne incidenten en alle incidenten. Het 'aantal gerapporteerde incidenten' gebruiken we als een samenvattende maat voor de (interne) criminaliteit waarmee deze bedrijven in de afgelopen drie jaar zijn geconfronteerd. We hebben voor deze maat gekozen vanwege de leesbaarheid. Het is echter ook mogelijk om andere maten te gebruiken, zoals het aantal *soorten* normovertredingen waarmee bedrijven te maken hebben gehad of een combinatiemaat (waarin verdisconteerd: aantal soorten normovertredingen én aantal incidenten). Deze alternatieve maten laten meestal dezelfde resultaten zien als welke zijn weergegeven in tabel 8. Wanneer ze afwijken, zullen we hiervan verslag doen. In een samenvattende maat zijn zeer uiteenlopende normovertredingen bijeengebracht. Het is mogelijk dat samenhangen tussen bedrijfskenmerken en individuele soorten normovertredingen afwijken van het 'algemene beeld'. Als dit het geval is, zullen we hiervan melding maken.

Tabel 8 Gemiddeld aantal gerapporteerde incidenten per bedrijf (totaal en intern) over de afgelopen drie jaar afgezet tegen kenmerken van bedrijven

(n=aantal bedrijven)	*Gemiddeld aantal incidenten (totaal) per bedrijf in drie jaar*	*Gemiddeld aantal interne incidenten per bedrijf in drie jaar*
Geografische ligging		
Regio Schiphol (18)	18	11
Regio Rotterdam (28)	11	6
Overige randstad (18)	25	16
Noord-Brabant/Limburg (41)	22	16
Elders in Nederland (34)	12	6

[27] De scores van extreem scorende bedrijven zijn naar beneden afgerond op maximaal honderd gemelde (interne) incidenten.

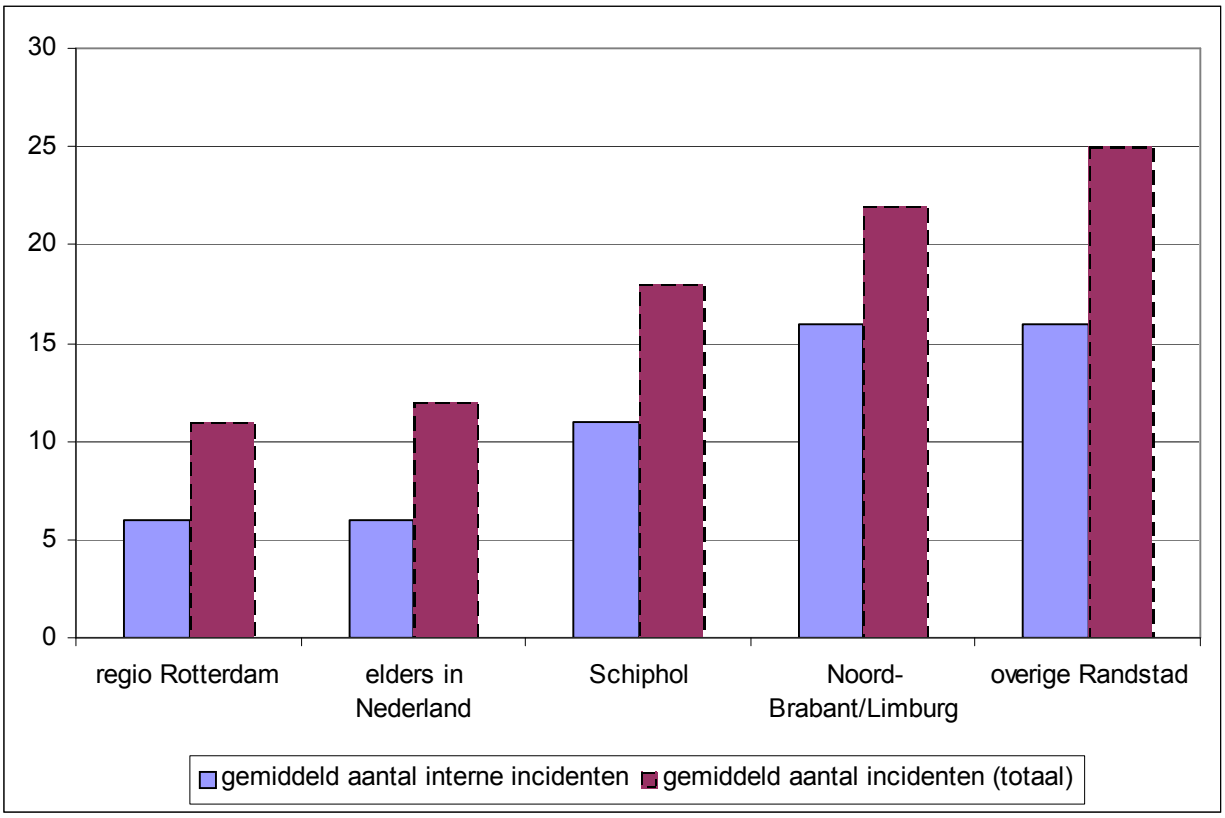
Omvang (in Nederland)		
Klein: < 50 werknemers (37)	11	6
Middelgroot: 50-200 werknemers (53)	15	9
Groot: > 200 werknemers (49)	24	17
Risicovolle goederen		
Producten met laagste risico (7)	7	5
Producten met middelgroot risico (53)	13	8
Producten met grootste risico (79)	21	14
Aard bedrijfsactiviteiten: % loodspersoneel		
0-25 procent (28)	25	15
26-50 procent (36)	20	14
51-75 procent (19)	12	9
76-100 procent (54)	13	8
Aard bedrijfsactiviteiten: transportfunctie		
Geen transport/uitbesteed (87)	14	8
Wel transport/deels uitbesteed (47)	24	17
Aanwezigheid van extern personeel in bedrijf		
Geen extern personeel aanwezig (17)	7	4
Wel extern personeel aanwezig (111)	19	12
Problemen met werven van 'goed' personeel		
Geen problemen (55)	13	6
Wel problemen (80)	21	15
Beveiligingsniveau		
Laag (16)	8	2
Middel (98)	19	12
Hoog (25)	18	14

4.1.1 Geografische ligging

De bedrijven in ons onderzoek zijn geconcentreerd op bepaalde plekken in Nederland: op Schiphol, in Rotterdam (haven en agglomeratie) en in Noord-Brabant/Limburg (met concentraties bedrijven in de agglomeraties van Moerdijk, Tilburg, Eindhoven en Venlo).
De overige ondernemingen zijn verspreid over Nederland, met een zekere concentratie in de grensstreek met Duitsland (lijn Nijmegen-Enschede). Veel bedrijven hebben meer dan één vestiging. De in tabel 8 gepresenteerde cijfers omtrent geografische indeling moeten, zoals al in hoofdstuk 2 is besproken, derhalve met enige voorbehouden worden geïnterpreteerd.[28]

Figuur 1 Gemiddeld aantal gerapporteerde (interne) incidenten per bedrijf naar regio (over laatste drie jaar)

[28] De reden dat we deze gegevens hier toch durven presenteren vloeit voort uit het feit dat enkele tests met alternatieve locatie-indelingen telkens vergelijkbare resultaten laten zien.



We hebben de relatie tussen geografische ligging en aantal gerapporteerde incidenten ook grafisch weergegeven in figuur 1. We zien een globaal verschil in gerapporteerde incidenten tussen de regio's Schiphol, (overige) randstad en Brabant/Limburg enerzijds en Rotterdam en de rest van Nederland anderzijds. In laatstgenoemde gebieden ligt het aantal incidenten beduidend beneden het niveau van de eerstgenoemde gebieden. Deze verschillen laten zich verklaren uit het feit dat de bedrijven in de betreffende regio's op enkele risicokenmerken van elkaar afwijken. Dit zijn kenmerken die ook elders in tabel 8 zijn genoemd en samenhang vertonen met het aantal gerapporteerde incidenten. Zo zien we dat de bedrijven op Schiphol afwijken doordat ze veel vaker dan bedrijven in de andere regio's de meest 'risicovolle' goederen behandelen. De bedrijven in Rotterdam hebben relatief weinig incidenten gerapporteerd. De achtergrond hiervan is deels dat het in deze regio relatief vaak gaat om kleine bedrijven (minder dan vijftig werknemers) die in veel gevallen ook geen eigen transport hebben. Zoals we verderop zullen zien, beperken deze kenmerken de risico's op (interne) criminaliteit. Ze kunnen echter niet helemaal verklaren waarom de Rotterdamse bedrijven zo 'laag scoren'. Dat de bedrijven in de rest van de randstad hoge scores laten zien, kan onder meer worden toegeschreven aan het feit dat het hierbij naar verhouding vaker gaat om grote ondernemingen (meer dan tweehonderd werknemers) die vaker dan de bedrijven in de andere regio's (een deel van) hun eigen transport regelen. Ook ligt bij deze bedrijven het percentage extern personeel relatief hoger (zoals uitzendkrachten, maar ook medewerkers van andere bedrijven die in of rond de betreffende bedrijven werkzaam zijn). De bedrijven in Brabant en Limburg wijken af doordat ze vaker dan bedrijven in andere regio's een relatief laag beveiligingsniveau kennen, terwijl de goederen die ze behandelen gemiddeld genomen even risicovol zijn. De bedrijven elders in Nederland wijken vooral af doordat ze veel minder vaak dan bedrijven in de eerdergenoemde regio's te maken hebben met personeelsproblemen (problemen met werving en verloop van personeel).
Als we kijken naar het soort incidenten waar bedrijven in deze regio's slachtoffer van worden, dan zien we ook enkele opvallende verschillen: de bedrijven op Schiphol rapporteren naar verhouding minder vaak inbraken (zowel extern als intern), terwijl de prevalentie van deze normovertreding in de andere regio's zo'n beetje overal op een gelijk niveau ligt. Incidenten die door bedrijven op Schiphol juist vaker dan gemiddeld worden gemeld zijn het ongeoorloofd privé gebruiken van bedrijfsmiddelen, vechtpartijen en illegale handel. De bedrijven in Rotterdam rapporteren naar verhouding vaker dat

medewerkers verwijtbaar nalatig zijn geweest bij het uitoefenen van hun werk. Hierbij gaat het vaak om chauffeurs en andere medewerkers die tegen de regels in bepaalde veiligheidsprocedures niet in acht hebben genomen, waardoor een misdrijf kon plaatsvinden (meestal verduistering van goederen). Op Schiphol wordt deze normovertreding juist relatief weinig gerapporteerd. Bedrijven in de rest van de randstad rapporteren vaker dan gemiddeld slachtofferschap van verduistering en inbraken waarbij sprake is van interne betrokkenheid. Bedrijven in Brabant en Limburg en in mindere mate ook elders in Nederland worden iets vaker dan gemiddeld geconfronteerd met sabotage-activiteiten van medewerkers. Normovertredingen zoals (interne) verduistering, fraude en vernieling komen zo'n beetje in alle regio's even vaak voor.

Met alle slagen om de arm die nodig zijn vanwege de gebruikte maat voor geografische indeling, kunnen we stellen dat er regionale verschillen bestaan naar aard en omvang van gerapporteerde interne criminaliteit. De bedrijven in de randstad en in Brabant en Limburg rapporteren meer interne problemen dan bedrijven buiten deze gebieden. Stedelijkheid speelt hierbij een rol. De meeste bedrijven in de genoemde regio's liggen in (groot)stedelijke gebieden, de bedrijven in de rest van Nederland juist vaker daarbuiten. Mede doordat de bedrijven in Rotterdam op enkele belangrijke (risico)kenmerken afwijken van de rest van de steekproef, vormen zij hierop een uitzondering. Ten slotte bestaan er ook verschillen in het soort incidenten waarmee bedrijven in deze regio's vaker of minder vaak te maken hebben. Sommige normovertredingen komen echter overal in ongeveer gelijke mate voor.

4.1.2 Omvang

We zien in tabel 8 dat grote bedrijven (met meer dan tweehonderd werknemers in Nederland) gemiddeld ruim twee tot drie keer zoveel (interne) incidenten melden als kleine bedrijven. Als zodanig lijkt (interne) criminaliteit dus een verschijnsel waarvan vooral grote bedrijven last hebben. Nu ligt het voor de hand dat in grote bedrijven meer incidenten plaatsvinden, omdat onze maat voor omvang is afgeleid van het aantal personeelsleden; hoe meer personeel des te meer 'potentie' voor interne criminaliteit. Er is echter meer aan de hand. Zoals al in hoofdstuk 2 naar voren kwam, is tijdens de interviews niet altijd de situatie in het bedrijf als geheel besproken, omdat respondenten in met name grotere bedrijven niet altijd (goed) zicht hadden op wat zich in het gehele bedrijf afspeelde. De correlatie tussen bedrijfsomvang en gerapporteerde incidenten blijft bestaan als we controleren voor deze factor. Omgekeerd verdwijnt de correlatie tussen het aantal vestigingen waarover gesproken is en het aantal gerapporteerde incidenten, wanneer we rekening houden met de omvang van het bedrijf als geheel. Met andere woorden, de omvang van de onderneming heeft, onafhankelijk van het aantal personeelsleden dat normovertredingen kan begaan, een effect op het aantal gerapporteerde incidenten: in vestigingen van grote ondernemingen worden meer (vooral interne) incidenten gemeld dan in vergelijkbare vestigingen van kleinere ondernemingen.[29]
Belangrijke verschillen tussen grote en kleine ondernemingen doen zich vooral voor bij verduistering. Dit wordt door 81% van de grote ondernemingen gerapporteerd tegen 35% bij de kleine ondernemingen (voor 'interne' verduistering liggen de percentages op respectievelijk 81% en 27%). Behalve verduistering is ook interne vernieling een normovertreding die vooral bij grote ondernemingen vóórkomt. Van de grote ondernemingen rapporteert 16% deze normovertreding. Door de kleine bedrijven wordt deze normovertreding geen enkele keer gerapporteerd. Bij inbraken is de variatie tussen grote en kleine bedrijven veel minder: 80% van de grote ondernemingen rapporteert dit tegen 70% van de kleine ondernemingen (bij 'interne' inbraken liggen de percentages op respectievelijk 47% en 30%). Ook ten aanzien van normovertredingen als overvallen, oplichting en sabotage van werkprocessen zijn de verschillen in gerapporteerde incidenten tussen grote en kleine

[29] Correlaties bivariaat:
- criminaliteit totaal/intern * omvang (r=.30/.36, p<.001)
- criminaliteit totaal/intern * aantal vestigingen bevraagd (r=.26/.25, p<.01).
Partiële correlaties:
- gecontroleerd voor aantal vestigingen bevraagd: criminaliteit totaal/intern * omvang (r=.19/.27, p<.05/p<.01)
- gecontroleerd voor omvang: criminaliteit totaal/intern * aantal vestigingen bevraagd (r=.09/.04, p=.30, p=.65).

bedrijven niet zo groot. Afwijkend van het algemene beeld is dat met name kleine bedrijven relatief vaak slachtoffer worden van zaken als fraude, privé-gebruik van bedrijfsmiddelen en (in mindere mate) nalatigheid van werknemers. Zo ligt bijvoorbeeld het percentage kleine bedrijven dat fraudegevallen rapporteert twee keer zo hoog als bij grote bedrijven.

Al met al kunnen we concluderen dat bedrijfsomvang is gerelateerd aan prevalentie en frequentie van interne criminaliteit. Deze relatie stijgt uit boven het getalsmatige gegeven dat meer medewerkers meer normovertredingen kunnen begaan. Grote bedrijven zijn ook 'intrinsiek' criminogener (dat wil zeggen 'vatbaarder' voor criminaliteit). Bij sommige vormen van interne criminaliteit wijkt het beeld echter af. Zo worden fraude, ongeoorloofd privé-gebruik van bedrijfsmiddelen en (in mindere mate) nalatigheid van werknemers naar verhouding juist vaker gemeld door kleine ondernemingen.

4.1.3 Risicovolle goederen

Het besluit om dit onderzoek te laten plaatsvinden in de logistieke sector had onder andere te maken met de verwachting dat deze sector 'last' heeft van het feit dat er voortdurend grote hoeveelheden zeer diefstalgevoelige goederen in omgaan. Het ligt dan ook voor de hand om te onderzoeken in hoeverre de aanwezigheid van 'risicovolle' goederen samenhangt met gerapporteerde incidenten.
We zien in tabel 8 dat de aanwezigheid van risicovolle goederen inderdaad een sterk criminaliteitsverhogend effect heeft: het aantal gerapporteerde (interne) incidenten ligt in de bedrijven met de meest risicovolle goederen (bijna) drie keer hoger dan in bedrijven met laagwaardige goederen. De kans op overvallen neemt sterk toe bij risicovollere goederen. Zo meldt 23% van de bedrijven met de meest risicovolle goederen dat ze in de afgelopen drie jaar eenmaal of vaker slachtoffer is geworden van een overval tegen respectievelijk 4% en 0% bij de andere bedrijven. Bij inbraken en verduisteringen zijn de verschillen kleiner, maar ook hier neemt de kans erop toe naarmate sprake is van meer risicovolle goederen. Ook illegale handel en vechtpartijen worden vaker gerapporteerd in bedrijven met de meest risicovolle goederen. Dit heeft wellicht te maken met het feit dat deze bedrijven gemiddeld ook groter zijn. Fraudegevallen zijn *niet* gerelateerd aan de aanwezigheid van risicovolle goederen.

Samenvattend: de aanwezigheid van risicovolle goederen vergroot de kans op (interne) criminaliteit in bedrijven.

4.1.4 Behandeling van goederen

Behalve het soort goederen waarmee bedrijven werken, kan ook de behandeling van deze goederen zijn gerelateerd aan het fenomeen interne criminaliteit (niet weergegeven in tabel 8). We hebben eerst gekeken of bedrijven die alleen aan op- en overslag van goederen doen, verschillen van bedrijven die 'iets' met de goederen doen, zoals groupage, orderpicken, verpakken, stickeren, assembleren, repareren of andere VAL-activiteiten. Dit onderscheid blijkt niet relevant voor het rapporteren van incidenten. Hierbij moet worden opgemerkt dat de overgrote meerderheid van de bedrijven in de steekproef méér doet met de goederen dan alleen op- en overslaan. Vervolgens hebben we gekeken of de afzonderlijke activiteiten (orderpicken, et cetera) mogelijk relevant zijn voor het rapporteren van incidenten. Ook dat blijkt niet het geval.

Al met al hebben we dus geen betekenisvol verband kunnen vinden tussen de behandeling van goederen en de aard en omvang van de gerapporteerde (interne) criminaliteit. Door verschillende bedrijven is echter opgemerkt dat zij bepaalde activiteiten -op grond van ervaringen in het verleden- beschouwen als risicovol, bijvoorbeeld orderpicking, assemblage en andere activiteiten waarbij de goederen op stuks- of doosniveau door de handen van medewerkers gaan. Het lijkt echter erop dat onze steekproef op dit punt te homogeen is om een verband aan te kunnen treffen; bijna alle bedrijven in ons onderzoek doen 'iets' met de goederen die ze onder hun beheer hebben.[30]

[30] Dit is ook niet vreemd, want het was een selectiecriterium bij de samenstelling van de steekproef.

4.1.5 Aard van bedrijfsactiviteiten

Naast het soort goederen en de bewerkingen die erop plaatsvinden, kan ook de aard van de bedrijfsactiviteiten gerelateerd zijn aan de aard en omvang van de gerapporteerde incidenten. We zagen in het vorige hoofdstuk al dat hierbij een belangrijk onderscheid aan de orde is tussen *transportgerelateerde* criminaliteit en *loodsgerelateerde* criminaliteit.
In tabel 8 hebben we het percentage van het personeel weergegeven dat werkzaam is in of ten behoeve van de loods (ten opzichte van personeel dat werkzaam is in of ten behoeve van het transport of andere activiteiten). We zien dat het aantal gerapporteerde interne incidenten afneemt naarmate een groter deel van het personeel loodsgerelateerd werkzaam is. Een geringer aandeel van het loodsgerelateerd personeel betekent bijna altijd dat een groter deel van het personeel transportgerelateerd werkzaam is. Deze bevinding wordt bevestigd door het feit dat bedrijven die geen eigen transportfunctie hebben of die het transport geheel hebben uitbesteed, gemiddeld genomen veel minder (interne) incidenten melden dan bedrijven die wel een eigen transportfunctie hebben. Het is evident, ook uit de gesprekken bij de bedrijven, dat zij het transport als de grootste risicofactor zien voor criminaliteit.
Als we kijken naar specifieke vormen van (interne) criminaliteit, dan zien we dat inbraken (inclusief ladingdiefstallen) vaker aan de orde zijn in bedrijven die (veel) aan transport doen: 92% van de bedrijven met een eigen transportfunctie rapporteert deze incidenten tegen 68% van de bedrijven die geen eigen transportfunctie hebben (of deze volledig hebben uitbesteed). Ook illegale handel en nalatigheid door medewerkers wordt vaker gemeld door bedrijven met een eigen transportfunctie. Verduistering daarentegen wordt iets vaker gemeld door bedrijven wier personeel voor het grootste deel werkzaam is in de loods. De verschillen zijn hier echter kleiner (72% van de bedrijven met meer dan driekwart loodsgerelateerd personeel maakt melding van verduistering tegen 53% van de bedrijven met minder dan een kwart loodsgerelateerd personeel).

Samenvattend kunnen we stellen dat transportactiviteiten meer gerelateerd zijn aan (interne) criminaliteit dan loodsactiviteiten. Het gaat hierbij vooral om inbraken (zijnde trailer- en ladingdiefstallen). Verduisteringen worden daarentegen vaker gerapporteerd door bedrijven wier personeel voor het grootste deel werkzaam is in de loods.

4.1.6 Aanwezigheid van extern personeel in bedrijf

Een veelvoorkomende gedachte, ook bij de respondenten in ons onderzoek (zie hiervoor ook paragraaf 5.2), is dat uitzendkrachten en ander ‘extern’ personeel een verhoogd risico opleveren voor interne criminaliteit. In het onderzoek hebben we bedrijven gevraagd in hoeverre zij te maken hebben met extern personeel dat toegang heeft tot het bedrijf. Hierbij gaat het in de meeste gevallen om uitzendkrachten, maar het kan ook gaan om medewerkers van andere bedrijven die ter plaatse hun werk verrichten, zoals chauffeurs, loodsmedewerkers die in dienst zijn van een opdrachtgever, externe onderhoudsmonteurs, schoonmakers, ICT-specialisten die het computernetwerk onderhouden, et cetera. De bedrijven die niet of nauwelijks te maken hebben met extern personeel rapporteren inderdaad aanzienlijk minder incidenten dan bedrijven die hiermee wel te maken hebben. We zien echter dat het aantal bedrijven zonder extern personeel tamelijk gering is (13%). Nadere analyse van deze gegevens laat zien dat de bedrijven zonder extern personeel op een belangrijk risicokenmerk afwijken van bedrijven mét extern personeel: het gaat meestal om kleine bedrijven (gemiddeld 65 personeelsleden), terwijl de bedrijven mét extern personeel gemiddeld 280 werknemers hebben. Controleren we voor de omvang van de onderneming, dan verdwijnt voor een belangrijk deel de samenhang tussen de aanwezigheid van extern personeel en het aantal gerapporteerde incidenten.[31]

Samenvattend: we kunnen wel een samenhang waarnemen tussen de aanwezigheid van extern personeel in een bedrijf en het aantal gerapporteerde incidenten, maar deze samenhang kan in belangrijke mate worden verklaard uit het feit dat met name grotere bedrijven gebruik maken van extern personeel.

[31] Omgekeerd is dit niet het geval: de correlatie tussen omvang van de onderneming en het aantal gerapporteerde incidenten blijft bestaan nadat we controleren voor de aanwezigheid van extern personeel in het bedrijf.

4.1.7 Problemen met personeel

We hebben bedrijven gevraagd in hoeverre ze problemen hebben met het werven van goed personeel en hoe het staat met het verloop van personeel in het bedrijf. Bijna zes op de tien bedrijven meldden ons problemen te hebben (gehad) met het werven van goed personeel. Hierbij gaat het soms om een krappe arbeidsmarktsituatie, maar vaker noemen bedrijven niet zozeer de beschikbaarheid van personeel als een probleem, als wel de kwaliteit en betrouwbaarheid van het beschikbare personeel. Hierbij gaat het meestal om operationele functies zoals chauffeurs, loodsmedewerkers en planners. Sommige bedrijven gaven aan op alle niveaus in de organisatie met wervingsproblemen te kampen hebben.
We zien in tabel 8 dat bedrijven die problemen hebben met de werving van goed personeel, meer incidenten, vooral ook meer interne incidenten, rapporteren dan bedrijven die zeggen geen wervingsproblemen te hebben. Hetzelfde geldt voor het verloop van personeel (niet in tabel 8 gepresenteerd): bedrijven met een groot personeelsverloop rapporteren aanzienlijk meer interne incidenten dan bedrijven met een gering verloop. Bij een aantal bedrijven hangen deze verschijnselen ook samen. Deze bedrijven hebben te maken met zowel wervingsproblemen als met een groot verloop (dit is echter lang niet altijd aan de orde!). We hebben eerder gezien dat problemen met de werving van goed personeel zich in sterkere mate voordoen in de randstad en in Brabant en Limburg, dan in de rest van Nederland. Dit geldt ook voor het verloop van personeel. Problemen met personeel zijn niet gerelateerd aan andere (risico)kenmerken van bedrijven.
Het is de vraag welke betekenis we aan dit verband moeten toekennen. Als we afgaan op de respondenten spelen hierbij zowel vraag- als aanbodfactoren een rol. Enerzijds maakten respondenten melding van het feit dat veel -potentieel- personeel onvoldoende kwaliteiten heeft (bijvoorbeeld gebrekkige beheersing van het Nederlands, onvoldoende diploma's), een verkeerde instelling heeft (niet gemotiveerd) of niet betrouwbaar is (in de zin van aanwezig zijn, inzet en dergelijke). Anderzijds meldden ze ons dat ze hoge eisen stellen aan hun personeel (ook als het gaat om laagbetaalde banen) en dat de vacatures die ze moeilijk kunnen vervullen niet altijd even aantrekkelijk zijn als het gaat om arbeidsomstandigheden (zwaar werk, lang van huis, matige betaling). Wij geloven dat beide factoren hier een rol spelen. Uit het feit dat bedrijven in de meest stedelijke gebieden meer problemen hebben met het werven (en vasthouden) van personeel dan bedrijven buiten deze gebieden, zien we een bevestiging van de eerste factor. Dat ook de arbeidsomstandigheden van belang zijn, zagen we tijdens de interviews meermalen bevestigd door het feit dat bedrijven die juist weinig problemen op dit vlak ervaren dit vaak toeschreven aan het feit dat de primaire en secundaire arbeidsomstandigheden in het bedrijf boven die van de concurrenten lagen.
Als we kijken naar de afzonderlijke normovertredingen zien we dat zaken als fraude, sabotage van werkprocessen, vernieling, vechtpartijen, ongeoorloofd privé-gebruik van bedrijfsmiddelen, maar ook het doorspelen van gevoelige bedrijfsinformatie, (veel) vaker voorkomen in bedrijven die personeelsproblemen hebben. Zo meldt bijvoorbeeld 23% van deze bedrijven fraudegevallen (tegen 11% in de groep bedrijven die geen personeelsproblemen heeft). Nog opvallender is dat 18% van deze bedrijven meldt dat medewerkers wel eens vertrouwelijke bedrijfsinformatie hebben doorgespeeld aan concurrenten (tegen slechts 4% bij de andere bedrijven). Het rapporteren van nalatigheid van personeel is níet gerelateerd aan personeelsproblematiek, evenals verduisteringen: bedrijven mét en zonder personeelsproblemen rapporteren opvallend genoeg even vaak slachtofferschap van verduistering. Frappant is ook dat bedrijven met personeelsproblemen vaker externe incidenten zoals overvallen en inbraken melden (respectievelijk 19% tegen 6% en 84% tegen 67%). Als we vervolgens kijken in hoeverre hierbij volgens de bedrijven sprake is van interne betrokkenheid, dan verdwijnen de verschillen, met andere woorden: bedrijven mét en zonder personeelsproblemen rapporteren ongeveer even vaak interne overvallen en inbraken.

Samenvattend kunnen we opmerken dat problemen die bedrijven hebben met de werving (en ook het verloop) van personeel gerelateerd zijn aan de mate waarin deze bedrijven te maken hebben met interne criminaliteit. Deze problemen kunnen duiden op minder gunstige arbeidsomstandigheden in het bedrijf, maar ook op de aanwezigheid van personeel met een verhoogd risico (ten aanzien van interne criminaliteit). Opvallend is dat genoemde personeelsproblemen ook gerelateerd zijn aan

bepaalde vormen van externe criminaliteit, zoals overvallen en inbraken. Als we deze bevinding relateren aan het besprokene in paragraaf 3.5 is het niet onaannemelijk om te veronderstellen dat bij tenminste een deel van de externe overvallen en inbraken sprake is geweest van interne betrokkenheid.

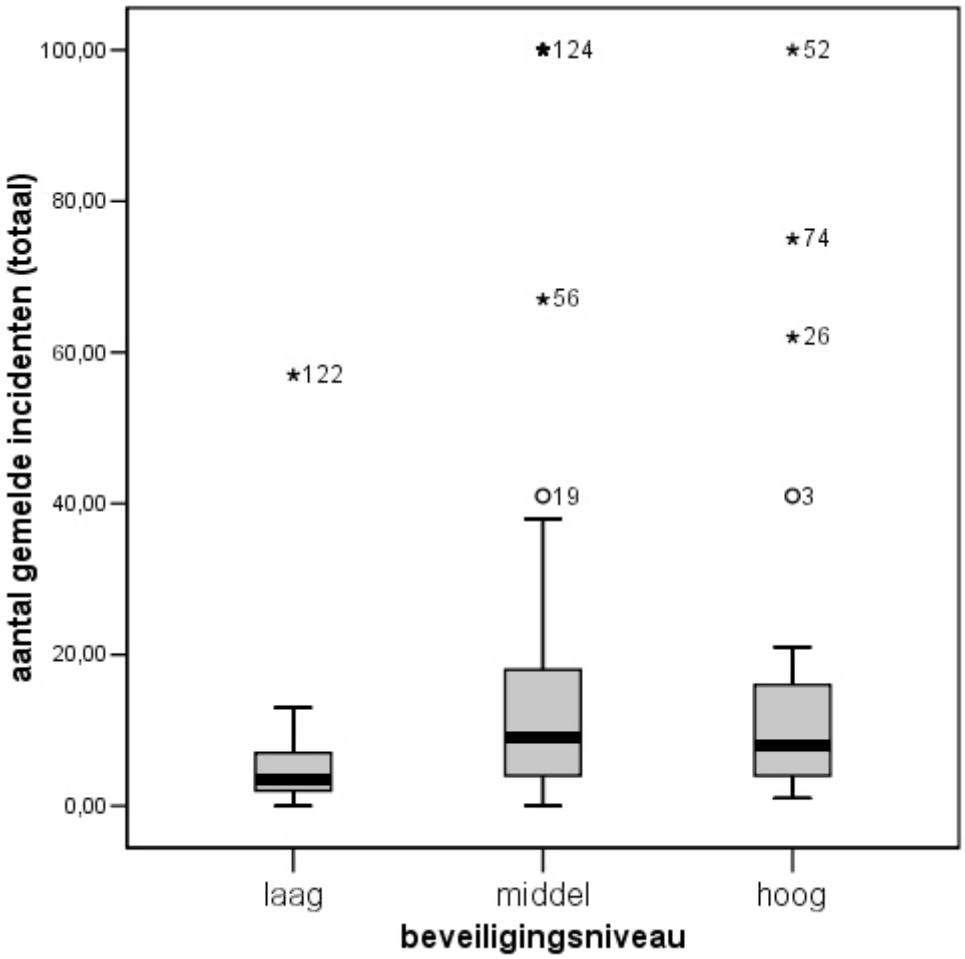
4.1.8 Beveiligingsniveau

Het ligt voor de hand te veronderstellen dat beveiligings- en preventiemaatregelen van invloed zijn op het aantal gerapporteerde incidenten. We hebben de bedrijven een reeks van preventiemaatregelen en -activiteiten voorgelegd en gevraagd of deze in hun bedrijf vóórkomen. Zoals in hoofdstuk 5 uitgebreid zal worden besproken, kan worden afgeleid dat een kleine groep bedrijven een laag tot zeer laag beveiligingsniveau heeft (12%). Een hele grote groep bedrijven heeft een middelmatig beveiligingsniveau (70%) en een kleinere groep (18%) heeft een hoog tot zeer hoog beveiligingsniveau.
We zien in tabel 8 het paradoxale gegeven dat middelmatig en hoog beveiligde bedrijven veel meer incidenten rapporteren dan laag beveiligde bedrijven. Bij het rapporteren van interne incidenten is het verschil zelfs opvallend groot. Als we de alternatieve maten voor (interne) criminaliteit erbij betrekken, zien we dat vooral bij het rapporteren van interne incidenten er een lineair verband bestaat met het beveiligingsniveau. Zo rapporteren laag beveiligde bedrijven gemiddeld 1,25 *soorten* interne normovertredingen, middelmatig beveiligde bedrijven rapporteren gemiddeld 2,18 *soorten* interne normovertredingen en hoog beveiligde bedrijven rapporteren gemiddeld 2,84 *soorten* interne normovertredingen. Bij het rapporteren van externe criminaliteit (volgens de alternatieve maten) lijkt het beeld op het gerapporteerde in tabel 8, dat wil zeggen: bedrijven met een laag beveiligingsniveau rapporteren de minste criminaliteit, bedrijven met een middelmatig beveiligingsniveau rapporteren de meeste criminaliteit en bedrijven met een hoog beveiligingsniveau liggen qua gerapporteerde criminaliteit net onder de middelmatig beveiligde bedrijven.
Het paradoxale gegeven dat beter beveiligde bedrijven meer incidenten rapporteren, laat zich verklaren vanuit de ervaring dat bedrijven heel vaak hun beveiliging (pas) opschalen naar aanleiding van incidenten waarmee ze te maken hebben gehad (voor een uitvoerige beschrijving hiervan zie hoofdstuk 5). Het beveiligingsniveau is daarmee een soort indicator van criminaliteitsproblemen. Immers, beveiliging kost geld en bedrijven zullen dit alleen uitgeven als de baten hiervan de lasten (schade door criminaliteit, niet in aanmerking komen voor bepaalde opdrachten, te dure verzekeringspolissen en dergelijke) overtreffen. Dus rapporteren bedrijven met een *security* manager meestal meer incidenten dan bedrijven zonder een specifieke veiligheidsfunctionaris en rapporteren bedrijven die voldoen aan de hoogste beveiligingseisen (TAPA) meer incidenten dan bedrijven die hier niet aan voldoen.
Op basis van een *cross section* onderzoek zoals het onderhavige, is het derhalve niet goed mogelijk om betrouwbare uitspraken te doen over het effect van preventiemaatregelen op (interne) criminaliteit in bedrijven. Er valt echter wel iets over te zeggen: in figuur 2 presenteren we voor elke groep bedrijven (laag, middel en hoog beveiligd) boxplots.[32] Hieruit kunnen we afleiden hoe de scores (op het aantal gerapporteerde incidenten) in deze groepen verdeeld zijn. Aan de ene kant zien we laag beveiligde bedrijven, die relatief weinig incidenten rapporteren. De spreiding van de scores in deze groep is gering. Aan de andere kant zien we hoog beveiligde bedrijven die gemiddeld meer incidenten rapporteren. De variatie tussen bedrijven die weinig en veel incidenten rapporteren is hier groter. De grootste spreiding zien we echter bij de middelmatig beveiligde bedrijven. Het zijn de hoog-scorende bedrijven die hier het gemiddelde (en de mediaan) omhoog trekken. Het lijkt er dus op dat de hoog beveiligde bedrijven, beter dan de middelmatig beveiligde bedrijven, in staat zijn om te voorkómen dat er heel veel incidenten plaatsvinden. Dit is temeer het geval wanneer we bedenken dat deze (hoog

[32] De spreiding van de scores kan worden afgeleid uit de lengte van de box (de interquartiele afstand: scores gelegen tussen het 25e en het 75e percentiel) en de lengte van de lijn (dit is de afstand tussen de laagste en de hoogste score met uitzondering van outliers en extreme scores). Outliers (o) zijn cases die 1,5 tot 3 boxlengten verwijderd liggen van elk einde van de box. Extreme scores (*) zijn cases die meer dan 3 boxlengten verwijderd liggen van elk eind van de box. De nummers bij de outliers en extreme waarden zijn casenummers van bedrijven uit de steekproef. De dikke horizontale streep in de box is de mediaan. De scores zijn gemaximeerd op maximaal 100 incidenten per bedrijf.

beveiligde) bedrijven ook nog eens vaker met risicovolle goederen werken dan bedrijven die middelmatig beveiligd zijn.

Figuur 2 Gerapporteerde criminaliteit afgezet tegen beveiligingsniveau in bedrijven (boxplots)



Als het gaat om interne incidenten zagen we in tabel 8 al dat hoog beveiligde bedrijven meer gevallen rapporteren dan middelmatig beveiligde bedrijven. We kunnen niet uitsluiten dat hierin ook een rapportage-effect tot uiting komt: hoog beveiligde bedrijven hebben doorgaans betere instrumenten om interne criminaliteit te monitoren en hebben doorgaans ook minder moeite om hiervan melding te maken aan onderzoekers. Overigens zien we ook hier weer terug dat met name in de groep van middelmatig beveiligde bedrijven de variatie tussen bedrijven die weinig interne incidenten rapporteren en bedrijven die heel veel incidenten rapporteren het grootst is.
Als we kijken naar het verband tussen beveiligingsmaatregelen en het rapporteren van afzonderlijke soorten normovertredingen, zien we een beeld dat in grote lijnen vergelijkbaar is met het onderscheid tussen kleine en grote ondernemingen: Het zijn vooral (interne) verduisteringen die door de best beveiligde bedrijven het meest gemeld worden (84% tegen 62% en 18% in de andere twee groepen). De verschillen bij inbraak zijn kleiner. Hier doet zich een interessant verschijnsel voor: de best beveiligde bedrijven rapporteren het minst vaak inbraken (68% tegen 80% en 75% bij de andere bedrijven), maar het vaakst ‘interne’ inbraken (44% tegen 32% en 35%). Het is opvallend dat de hoog-beveiligde bedrijven relatief vaker een ‘interne’ inbraak rapporteren, terwijl ze over de hele linie juist minder vaak inbraken rapporteren. In het vorige hoofdstuk hebben we gezien dat de kwalificatie ‘intern’ vooral een indicatie geeft van de kennis die bedrijven over het incident hebben. Het lijkt dus erop dat deze bedrijven door hun hoge beveiligingsniveau vaker in staat zijn om interne betrokkenheid bij een inbraak (of ladingdiefstal et cetera) aan te tonen. Het feit dat deze bedrijven ook vaker

verduistering rapporteren, bevestigt dit beeld. We hebben immers in het vorige hoofdstuk gezien dat het definiëren van gebeurtenissen als verduistering ook een zekere inspanning vereist van bedrijven.

Samenvattend concluderen we dat het beveiligingsniveau vooral een indicatie geeft van de criminaliteitsproblemen waarmee bedrijven te maken hebben. Immers, het opschalen van de beveiliging volgt heel vaak nadat het bedrijf is getroffen door incidenten (hierbij spelen ook andere factoren een rol, zie hoofdstuk 5). Het is voor ons dus moeilijk om uitspraken te doen over de effectiviteit van preventiemaatregelen. Met name in de groep van middelmatig beveiligde bedrijven zien we een grote variatie in gerapporteerde (interne) incidenten. Het lijkt erop dat de best beveiligde bedrijven er beter in slagen zeer hoge niveaus van (interne) criminaliteit tegen te gaan. Opvallend is verder dat de best beveiligde bedrijven vaker dan andere bedrijven met name interne (betrokkenheid bij) incidenten melden. Wij vermoeden dat hierbij ook sprake is van een rapportage-effect: deze bedrijven 'zien' meer interne criminaliteit dan minder beveiligde bedrijven.

4.2 Kenmerken van daders van interne criminaliteit

Gegevens over daders van interne criminaliteit zijn afkomstig van onze respondenten en weerspiegelen daarom vooral hún ervaringen met verdachten van interne criminaliteit. Zoals we in het vorige hoofdstuk hebben gezien, komen bepaalde vormen van interne criminaliteit in bedrijven eerder aan het licht dan andere. Ook tussen bedrijven variëren de mogelijkheden en inspanningen om concrete verdachten op het spoor te komen. Deze zaken zijn uiteraard van invloed op de rapportage. We hebben de respondenten in de bedrijven de algemene vraag voorgelegd of zij concrete verdachten van interne criminaliteit kennen of hebben gekend. Als dit het geval was, hebben we vervolgens gevraagd of ze iets meer over deze personen konden vertellen. In het bijzonder ging het ons hierbij om mogelijk gemeenschappelijke kenmerken in de persoonlijke achtergrond van deze personen of in hun relatie tot het bedrijf. Iets minder dan de helft van de respondenten (49%) kende één of meer concrete verdachten, gemiddeld dertien per persoon (dit getal wordt sterk vertekend doordat enkele respondenten uit hoofde van hun functie hiermee heel vaak te maken hadden).[33]
We hebben ook gegevens verzameld over individuele verdachten, naar aanleiding van specifieke incidenten die we met de respondenten hebben besproken. Hierbij gaat het in totaal om 141 personen die verdacht werden van zaken als verduistering (48), fraude (18), inbraak (16), verbaal of fysiek geweld (8), sabotage van bedrijfsprocessen (7) en een reeks van andere normovertredingen (telkens enkele verdachten per normovertreding). Deze selectie kwam tot stand doordat we bij het bespreken van de afzonderlijke normovertredingen telkens aan de respondenten vroegen om iets meer te vertellen over het laatste *interne* incident. In sommige gevallen was van dit incident ook een concrete verdachte bekend. Dit zijn de 141 hier genoemde personen.

4.2.1 Persoonlijke achtergrondkenmerken

De volgende vier kenmerken zijn door respondenten in meer of mindere mate genoemd als het gaat om achtergrondkenmerken van daders van interne criminaliteit (in volgorde van het aantal keren dat ze zijn genoemd):

- Problemen in de privé-situatie (meest genoemd);
- Demografische kenmerken;
- Persoonlijkheidsproblemen;
- Criminele antecedenten (minst genoemd).

Het meest genoemd als factor bij de totstandkoming van interne normovertredingen is 'privé-problemen van de verdachte'. In veruit de meeste gevallen gaat het hierbij om geldproblemen, maar ook wel om andere sociale problemen, vooral in het gezin (zoals scheiding en dergelijke). In enkele gevallen werd ook melding gemaakt van verslavingsproblematiek bij de betrokken verdachten. Enkele

[33] Mediaan is 5, modus is 1 en 2.

respondenten maakten melding van het feit dat met name diefstallen in eerste aanleg uit geldnood kunnen voortkomen, maar dat het motief in de loop van de tijd kan veranderen als de dader merkt hoe gemakkelijk en lucratief het voor hem is.
Ook demografische kenmerken zijn heel vaak genoemd. Hierbij gaat het vooral om jonge mannen, lager opgeleiden en (in mindere mate) allochtonen. Dit zijn de meest genoemde kenmerken. Er werd in sommige gevallen ook wel melding gemaakt van het feit dat de daders vooral hoogopgeleide (dan wel slimme) witte mannen waren, maar dit betrof gevallen die waren gerelateerd aan specifieke vormen van criminaliteit zoals fraude, doorspelen van bedrijfsinformatie en dergelijke. Bij de eerste groep gaat het naar verhouding veel vaker om verduistering van goederen, sabotage van werkprocessen, vernieling, et cetera; incidenten waarbij de schade voor het bedrijf (per incident althans) doorgaans geringer is.
In iets mindere mate hebben respondenten melding gemaakt van wat we hier hebben aangeduid als persoonlijkheidsproblemen. Hierbij gaat het volgens de respondenten onder meer om personen met een gering ontwikkeld normbesef, bij wie het gevoel voor *mein* en *dein* niet goed is ontwikkeld, maar ook om personen die een discrepantie ervaren tussen behoeften en mogelijkheden en aldus op te grote voet (proberen te) leven. Een aparte categorie in dit verband zijn de roekeloze jongeren die uit verveling of voor de kick bedrijfsmiddelen vernielen, werkprocessen saboteren of anderszins onprofessioneel en voor het bedrijf schadelijk gedrag vertonen.
Niet zo vaak genoemd is het criminele verleden van een verdachte of het feit dat deze deel uitmaakt van een criminele subcultuur of een crimineel netwerk. Vaak komt een bedrijf er ook pas achter dat een medewerker een crimineel verleden heeft als een onderzoek tegen zo'n persoon gaat lopen in verband met criminele feiten (vaak naar aanleiding van geweldsincidenten). Er zijn wel voorbeelden van bedrijven waar georganiseerde criminele verbanden medewerkers hebben omgekocht of eigen mensen in het bedrijf hebben geplant om misdrijven te faciliteren, maar dit betreft incidentele meldingen.

4.2.2 Relatie tot het bedrijf

In dit kader zijn de volgende kenmerken door respondenten naar voren gebracht (wederom in volgorde van het aantal keren dat ze zijn genoemd):

- Kenmerken van het dienstverband (meest genoemd);
- Functiekenmerken;
- Functioneren van werknemer (minst genoemd).

Als het gaat om dienstverband springen twee observaties eruit. De meest genoemde categorie betreft de verzameling van uitzendkrachten, werknemers met een tijdelijk contract en werknemers die pas kort bij het bedrijf werken. Kortom, allemaal personen met een geringe binding aan het bedrijf. Daarnaast wordt echter ook melding gemaakt, zij het in mindere mate, van daders die al een langere periode als vaste medewerker bij het bedrijf in dienst zijn. Het lijkt erop dat deze laatste groep, indien actief, schadelijker is voor de bedrijven dan de eerste groep, omdat het volgens de betrokkenen vaker gaat om omvangrijke incidenten, waarbij de werknemers hun kennis van het bedrijf en vaak ook hun opgebouwde vertrouwenspositie hebben gebruikt om bijvoorbeeld de beveiliging of andere procedures te omzeilen. Het soms grenzeloze vertrouwen dat leidinggevenden en anderen schenken aan met name werknemers die langer in dienst zijn, is volgens sommige respondenten dan ook onterecht en gevaarlijk. Of zoals een respondent het bondig uitdrukte: 'vertrouwen is goed, controle is beter'. Een aparte categorie in dit verband zijn de werknemers die op hun laatste werkdag een grote slag slaan. Ook deze incidenten leveren voor bedrijven vaak grote(re) schades op.
De meeste respondenten die melding hebben gemaakt van functiekenmerken noemen vooral uitvoerend personeel op de werkvloer: chauffeurs, loods- en productiepersoneel, schoonmakers, et cetera. In mindere mate wordt melding gemaakt van werknemers in toezichthoudende of controlerende functies, waarbij soms ook sprake is van samenwerking met uitvoerend personeel. Ook hierbij gaat het overigens vaak om personeel 'op de werkvloer'. Ook wordt een enkele keer melding gemaakt van werknemers in specialistische of andere, doorgaans hogere, functies. Hierbij gaat het meestal om vormen van witteboordencriminaliteit.

Het onbehoorlijk functioneren van een medewerker, maar vooral onvrede over het bedrijf (bijvoorbeeld over het salaris of over andere werkomstandigheden) is ook een aantal keren genoemd door respondenten. Deze factoren worden vaak genoemd bij delicten als opzettelijke beschadiging van bedrijfsmiddelen en het doorspelen van gevoelige bedrijfsinformatie aan concurrenten. Wraak jegens het bedrijf wordt in deze gevallen vaak als motief genoemd. Overigens gaat het bij het laatste delict ook nog om een bijzondere categorie van ontevreden werknemers, namelijk de ontevreden *ex*-werknemers. Ook bij enkele andere normovertredingen komt de boze ex-werknemer soms om de hoek kijken (bijvoorbeeld bij bedreiging van personeel, bij afpersing en soms ook bij inbraak of verduistering).

4.2.3 Overige kenmerken

De volgende twee kenmerken zijn ook meermalen genoemd. Ze zijn niet exclusief verbonden met de persoonlijke eigenschappen van de dader of met hun relatie tot het bedrijf. Het zijn niettemin interessante kenmerken om hier te bespreken.

- De dader uit onverwachte hoek;
- Geen standaardkenmerken aan te wijzen/(gelegenheidsstructuur is bepalend).

De dader uit onverwachte hoek is vaak genoemd door respondenten van bedrijven die niet veel ervaring hadden met concrete verdachten van interne criminaliteit. In voorkomende gevallen was men zeer verbaasd over de persoon van de dader. Nu is het ons niet bekend welke ideeën en verwachtingen er zoal in deze bedrijven leven als het gaat om verdachten van interne criminaliteit, maar volgens opgave van deze respondenten zat het onverwachte vaak in het feit dat de daders voorbeeldige werknemers bleken te zijn die bijvoorbeeld veel inzet toonden, loyaal waren aan het bedrijf, er vaak al langer werkten en die verder nooit problemen veroorzaakten. Een vergelijkbare waarneming, maar nu vaker gedaan door respondenten die juist frequent met verdachten van interne criminaliteit te maken hebben, is dat er geen standaardkenmerken zijn aan te wijzen en dat iedere medewerker, ongeacht zijn achtergrond en functie, een mogelijke dader kan zijn. Deze ervaring duidt erop dat persoonlijke motieven, zoals hiervoor besproken, in (veel?) gevallen minder gewicht in de schaal leggen dan de criminogene eigenschappen van gelegenheidsstructuren waaraan werknemers zijn ‘blootgesteld’. Door een aantal respondenten is de gelegenheidsstructuur ook expliciet genoemd als de belangrijkste factor.

4.3 Bevindingen in het licht van eerder onderzoek

In de onderzoeksliteratuur die zich richt op de verklaring van interne criminaliteit in organisaties wordt doorgaans een onderscheid gemaakt tussen beïnvloedende factoren op drie niveaus (Robinson en Greenberg, 1998):

- Persoonlijke factoren (niveau van de dader);
- Microsociale factoren (sociale interacties in het bedrijf);
- Organisatiefactoren (kenmerken van het bedrijf).

Wellicht is het goed om hier volledigheidshalve ook een vierde factor aan toe te voegen, namelijk:

- Omgevingsfactoren (context waarbinnen bedrijf opereert).

In dit hoofdstuk zijn we ingegaan op persoonlijke factoren die gerelateerd zijn aan interne criminaliteit en op organisatiefactoren. Onze data zijn niet fijnmazig genoeg om uitspraken te kunnen doen over microsociale factoren. Deze blijven hier dan ook buiten beschouwing. Op de omgevingsfactoren komen we terug in hoofdstuk 7.

Persoonlijke factoren

Als we kijken naar de factoren die op persoonlijk niveau gerelateerd zijn aan het verschijnsel interne criminaliteit, zien we in ons onderzoek een breed scala aan kenmerken voorbijkomen, zoals privé-problemen, sociaaldemografische kenmerken als leeftijd en opleiding (vooral jonge mannen), persoonlijkheidsproblemen (gering normbesef, leven op te grote voet, roekeloos gedrag), duur van het dienstverband (zowel kort als lang in dienst is een risico), aard van de functie (uitvoerend, controlerend, management), crimineel verleden of criminele contacten en onvrede over het werk. Deze brede waaier van factoren die op persoonsniveau gerelateerd zijn aan interne criminaliteit, zien we ook terug in ander onderzoek.
Hoffmann Bedrijfsrecherche publiceert jaarlijks gegevens over de kenmerken van interne normovertreders (Hoffmann, 2000-2004).[34] Deze tonen in grote lijnen een zelfde beeld als hier gepresenteerd. Hoffmann rapporteert weliswaar naar verhouding vaker normovertreders met een leidinggevende achtergrond, maar we vermoeden dat deze bevinding wordt veroorzaakt door de selectie die plaatsvindt doordat bedrijven Hoffmann eerder inschakelen bij incidenten met een omvangrijke schade. Dit bureau rapporteert ook dat de motieven van de normovertreders meestal financieel zijn en dat het vaak gaat om mannen jonger dan 45 jaar.[35] Uit een gesprek dat wij hebben gevoerd met een projectmanager van Hoffmann komt echter een diffuser beeld naar voren. Er worden door deze respondent weliswaar bepaalde risicogroepen genoemd, zoals bijvoorbeeld mannen tussen de 35 en 45 jaar die vijftien tot twintig jaar in dienst zijn (34% van hun verdachten), maar tegelijkertijd ook uitzendkrachten, tijdelijke krachten en personeel dat juist heel kort in dienst is.
Elzinga en Klerks (1998: 43 e.v.) noemen in hun onderzoek de volgende daderkenmerken: het gaat om personen van alle leeftijdsgroepen en van alle functieniveaus, zowel uitzend- als vaste krachten. Zij concluderen dat er geen duidelijk profiel kan worden geschetst van werknemers die betrokken zijn bij interne criminaliteit. Ook de motieven van de daders zijn volgens dit onderzoek zeer uiteenlopend, niet alleen economisch (gericht op winstbejag), maar ook pragmatisch (men heeft het gestolen product - even- nodig), psychologisch (bijvoorbeeld kickgedrag), cognitief (vanuit berekening, bijvoorbeeld compensatie voor slechte werkomstandigheden) of psychosociaal (bijvoorbeeld een verslaving die gefinancierd moet worden).[36]
In de overzichtsstudie van het Australian Institute of Criminology (AIC, 2004: 35) wordt een hele rij kenmerken genoemd als risicofactoren voor interne criminaliteit, zoals: werknemers met een crimineel verleden, adolescenten of jong volwassenen, mannen, werknemers in relatieve armoede, werknemers met een gebrekkige normontwikkeling, werknemers met een verslavingsgeschiedenis of een persoonlijkheidsstoornis en werknemers in het bezit van vuurwapens.
Ook in andere overzichtstudies zien we hetzelfde beeld. Robinson en Greenberg (1998: 11 e.v.) noemen als factoren onder meer: persoonlijkheidskenmerken, demografische kenmerken (vooral jonge mannen in lager betaalde banen, vaak uitzend- of tijdelijke krachten, of kort in dienst) en onvrede over betaling of werkomstandigheden. Bovendien stellen zij dat het belang van diverse factoren weer varieert bij verschillende vormen van interne criminaliteit. Kort gezegd: de plegers van grootschalige fraude hebben doorgaans een andere achtergrond dan personen die werkprocessen saboteren. Niehoff en Paul (2000) noemen de volgende risicofactoren op persoonlijk niveau: jongeren die op enigerlei wijze economische druk ervaren en emotioneel onstabiel zijn, die ook weinig binding met de samenleving en/of met het bedrijf hebben, doorgaans nieuw zijn in het bedrijf of parttime werken en vaak ook ongetrouwd zijn. Verder verrichten ze vaak laagbetaald werk en zijn de normovertredingen in het bedrijf gerelateerd aan ander normovertredend gedrag buiten het bedrijf. Huiras et al. (2000) noemen als risicogroepen: jonge mannen, personen die onvrede hebben over het werk of de betaling en werknemers die geen binding ervaren met het bedrijf. Uit hun eigen onderzoek blijkt dat

[34] Hoffmann Bedrijfsrecherche is in Nederland het grootste bureau op het gebied van private bedrijfsrecherche met circa 900 tot 1000 interne organisatieonderzoeken per jaar. Deze hebben niet altijd betrekking op de logistieke sector.
[35] Overigens doet Hoffmann in haar openbare rapporten ook uitspraken over de relevantie van de duur van het dienstverband. Kort geformuleerd: het risico is het grootst als iemand nog niet zo lang in dienst is (korter dan enkele jaren), maar deze conclusie nemen wij niet over, omdat geen rekening wordt gehouden met de gemiddelde duur van een dienstverband. Wij leiden uit de door Hoffmann gepresenteerde gegevens af dat er geen enkele relatie bestaat tussen duur van het dienstverband en interne normovertreding.
[36] Zie in dit verband ook Wielenga (1992: 38 e.v.). Deze noemt naast economische motieven ook ideologische, psychologische en sociaal-maatschappelijke motieven.

werknemers met een duidelijk carrièrebelang ook minder geneigd zullen zijn tot 'misdragingen op het werk' (Huiras et al., 2000). Ook andere auteurs noemen een scala aan persoonlijke kenmerken en motieven die een rol spelen bij interne criminaliteit (Murphy, 1993; Cools, 1994; Greenberg, 1997; Giacalone, Riordan en Rosenfeld, 1997).

Op de vraag derhalve welke persoonlijke factoren relevant zijn, kunnen we niet anders antwoorden dan dat een heleboel factoren relevant zijn gebleken. Dit antwoord is echter paradoxaal, want hoe meer factoren relevant blijken, des te minder kunnen de afzonderlijke factoren relevant zijn (hun onderscheidende vermogen wordt immers geringer). Met Murphy (1993) en Robinson en Greenberg (1998) geloven we dan ook dat het weinig zinvol is om enkel naar persoonlijke achtergrondkenmerken te kijken, eenvoudigweg omdat ze als zodanig niet gerelateerd zijn aan verschijnselen van interne criminaliteit. Deze bevinding komt niet overeen met de ideeën die hierover bestaan in veel bedrijven; daar gelooft men juist dat interne problemen voornamelijk worden veroorzaakt door uitzendkrachten (of bijvoorbeeld externe chauffeurs) en dus kunnen worden voorkómen door de *bad guys* buiten de deur te houden.

Organisatiefactoren
In dit onderzoek zijn de volgende kenmerken relevant gebleken: de omvang van de onderneming (hoe groter, des te meer interne criminaliteit), problemen ten aanzien van werving en verloop van personeel (bij prevalentie meer interne criminaliteit), de aard van de bedrijfsactiviteiten (hoe meer transport, des te meer interne criminaliteit), de aanwezigheid van risicovolle goederen (indien aanwezig meer criminaliteit) en de geografische ligging (bedrijven in Rotterdam rapporteren minder interne criminaliteit).
Kenmerken als omvang en stedelijke ligging worden in de literatuur regelmatig genoemd als factoren die verband houden met het niveau van interne criminaliteit in een organisatie (NIPO, 2002; VNO-NCW, 2003; PWC, 2003; BCC, 2004).
Elzinga en Klerks (1998) noemen in hun studie de volgende factoren die op bedrijfsniveau gerelateerd zijn aan interne criminaliteit: *norm- en strafbaarstelling* (zijn er duidelijke normen of is er een grijs gebied?), *risico-objecten* (vooral goederen met een zekere waarde, die beweegbaar/verplaatsbaar zijn, niet te omvangrijk en gemakkelijk toegankelijk vormen aantrekkelijke doelwitten), *risicomiddelen* (situaties die middelen verschaffen, dat wil zeggen gelegenheid creëren voor interne criminaliteit, zoals gebrekkige procedures en ingewikkelde en lange leveringsketens), *interne en externe drempels* (bijvoorbeeld normen en waarden in de organisatie, maar ook beveiliging) en ten slotte kenmerken die verband houden met de *bedrijfsvoering* (bijvoorbeeld openheid over interne criminaliteit, duidelijkheid over grenzen, binding van werknemers met de organisatie, bedrijfsklimaat en -cultuur, procedures en controles en efficiencybeleid).
In Amerikaans onderzoek zijn onder andere de volgende factoren op het niveau van bedrijven in verband gebracht met interne criminaliteit: bureaucratische organisatiestructuur, gebrekkige communicatie, niet-integer leiderschap (bevordert criminaliteit bij ondergeschikten)[37] en het ontbreken van duidelijke normen (Robinson en Greenberg, 1998: 17). Volgens deze auteurs zijn de hier genoemde factoren echter nog onvoldoende onderzocht. Meer empirisch bewijs is er volgens hen voor de relatie tussen interne criminaliteit en de betaling door het bedrijf (slechte of als onrechtvaardig beleefde betaling hangt samen met een hoger niveau van interne criminaliteit). Niehoff en Paul (2000) noemen als belangrijkste factoren op bedrijfsniveau: een als oneerlijk ervaren beloningsstructuur (niet alleen financieel) in combinatie met een gebrek aan controlemechanismen. De eerste factor creëert de motivatie voor interne criminaliteit, de tweede creëert de gelegenheid.
Murphy (1993: 142 e.v.) stelt dat het vooral van belang is de interveniërende processen te ontdekken tussen bepaalde bedrijfsomstandigheden en de wijze waarop deze het plaatsvinden van interne criminaliteit bevorderen. Hij hecht hierbij een groot belang aan normstelling en -handhaving, omdat deze activiteiten volgens hem de beste voorspeller van interne criminaliteit zijn (en dus ook de beste

[37] Ook Cools (1994) en Wielenga (2002) noemen de invloed van mismanagement of knoeiende managers op normovertreding door ondergeschikten. In ons onderzoek hebben we hiervoor anekdotisch bewijs gevonden: in enkele bedrijven waarin het management op grote schaal gefraudeerd had, kampte ook de werkvloer met ernstige problemen op het gebied van interne criminaliteit.

preventiemethode). Bovendien is normatieve sociale controle de meest kosteneffectieve preventiemethode. Deze bevindingen sluiten, zoals we in het volgende hoofdstuk zullen zien, aan bij de bevindingen in dit onderzoek.
Ten slotte geeft ook Krause (2002: 35) aan dat de loyaliteit van werknemers niet alleen afhankelijk is van een vertrouwensrelatie, maar ook van een groot aantal andere factoren waaronder de balans tussen werk en vrije tijd, de organisatiecultuur, carrièremogelijkheden en tevredenheid over het werk (Krause, 2002: 35).

Het onderhavige onderzoek biedt onvoldoende mogelijkheden om al deze verklarende factoren te toetsen, maar uit onze studie komt wel duidelijk naar voren dat de aanwezigheid van risicovolle goederen een (sterk) criminaliteitsverhogend effect heeft. Dit geldt eveneens voor problemen die het bedrijf ervaart met werving en selectie van personeel. Eén verklaring voor dit laatste is dat de arbeidsomstandigheden in bedrijven die hier problemen ondervinden door de betrokken werknemers niet als gunstig worden beschouwd. Deze bevinding vertoont een zekere overeenkomst met de bevinding uit het onderzoek van Elzinga en Klerks (1998) dat het werkklimaat in met name distributiebedrijven vaak te wensen over laat.[38]

4.4 Samenvatting en conclusie

Bedrijfskenmerken gerelateerd aan interne criminaliteit
In het voorafgaande is duidelijk geworden dat er verschillende bedrijfskenmerken gerelateerd zijn aan de aard en omvang van interne criminaliteit in bedrijven. In zijn algemeenheid zien we dat de volgende factoren het sterkst gerelateerd zijn aan het criminaliteitsniveau in bedrijven (in volgorde van belangrijkheid):[39]

- *Omvang* van het bedrijf (hoe groter des te meer criminaliteit);
- *Problemen met werving* van personeel (bij prevalentie meer criminaliteit);
- Aard bedrijfsactiviteiten (hoe meer *transportgerelateerd*, des te meer criminaliteit);
- Aanwezigheid van *hoog-risicovolle goederen* (bij aanwezigheid meer criminaliteit);
- Gevestigd in *Rotterdam* (deze bedrijven rapporteren minder criminaliteit)

We zien twee opvallende factoren. De eerste opvallende factor is ‘problemen met werving’. Deze problematiek blijkt, ook na uitschakeling van de invloed van de andere risicofactoren, gerelateerd aan het criminaliteitsniveau in een bedrijf, dus ook de ‘externe’ criminaliteit (waarbij het vooral gaat om overvallen en inbraken/ladingdiefstallen). Gelet op het besprokene in het vorige hoofdstuk (paragraaf 3.5) zien we hierin opnieuw een aanwijzing dat een deel van de door bedrijven als extern aangeduide criminaliteit wellicht een interne component heeft. Dat bedrijven in Rotterdam significant minder (interne) criminaliteit rapporteren kan niet helemaal worden verklaard door het feit dat de door ons onderzochte bedrijven in deze regio doorgaans klein zijn en weinig aan transport doen. Op de andere risicofactoren wijken deze bedrijven niet af van bedrijven elders in Nederland. Weliswaar scoren de Rotterdamse respondenten gemiddeld (iets) hoger op sociaal gewenst antwoordgedrag (dat wil zeggen dat ze naar de mening van de interviewers vaker incidenten onderrapporteren of beveiliging overrapporteren), maar de verschillen met de andere regio’s zijn niet heel groot. We hebben dan ook geen sluitende verklaring voor deze bevinding.

[38] Het onderzoek van Elzinga en Klerks had betrekking op 3 sectoren: naast de distributiesector ging het om de detailhandel en om ziekenhuizen.
[39] Deze bevinding is gebaseerd op een multivariate regressie-analyse, waarbij alle kenmerken uit tabel 4.1 (+ als controlefactor: het aantal vestigingen waar elk interview betrekking op had) zijn gebruikt als predictoren voor een samenvattende maat van criminaliteit (waarin verdisconteerd aantal soorten normovertredingen én aantal gerapporteerde incidenten). Van sommige kenmerken (zoals regio, risicovolle goederen) zijn dummy’s gemaakt. Van de andere kenmerken zijn de oorspronkelijke (ratio)scores gebruikt. Er is een *stepwise* regressie uitgevoerd. De volgorde van belangrijkheid is derhalve gebaseerd op de bijdrage van de afzonderlijke factoren aan de verklaarde variantie. Het model als geheel heeft een verklaarde variantie van R^2=.27.

De relaties van de andere bedrijfskenmerken met criminaliteit die in tabel 8 zijn genoemd, blijken niet stand te houden wanneer we rekening houden met de invloed van voornoemde factoren. Het gaat dan om zaken als beveiligingsniveau en de aanwezigheid van extern personeel in het bedrijf.[40] Dit hoeft, zoals we gezien hebben, niet te betekenen dat ze geen relevantie hebben voor het verschijnsel. Zo is bijvoorbeeld de aanwezigheid van extern personeel gerelateerd aan de omvang van de onderneming. Deze laatste factor blijkt bepalender voor de relatie met het aantal gerapporteerde (interne) incidenten. Het is uiteraard niet uitgesloten dat de aanwezigheid van extern personeel als 'bestanddeel' van de omvang van een onderneming hierbij een rol speelt. In een kwantitatieve analyse zoals wij hier hebben uitgevoerd, verdwijnt deze factor echter uit beeld. Een andere reden waarom bedrijfskenmerken nog wel relevant kunnen zijn terwijl ze niet in bovenstaand rijtje worden genoemd, is dat deze kenmerken weliswaar niet gerelateerd zijn aan (interne) criminaliteit in het algemeen, maar wel aan specifieke vormen ervan.
Als het specifiek om interne criminaliteit gaat, zien we nog wel een significante relatie tussen beveiligingsniveau en aantal gerapporteerde incidenten. De relatie tussen beveiligingsniveau en aantal gerapporteerde interne incidenten is een paradoxale, omdat hogere beveiligingsniveaus doorgaans samengaan met hogere niveaus van interne criminaliteit. Dit kan worden verklaard uit het feit dat veel bedrijven hun beveiliging opschalen naar aanleiding van incidenten. Over het effect van beveiliging op interne criminaliteit valt door ons dan ook weinig te zeggen. Wel zien we dat de best beveiligde bedrijven in ieder geval erin slagen te voorkómen dat ze geconfronteerd worden met hele hoge niveaus van interne criminaliteit.

Verplaatsing van criminaliteit
Bedrijven noemen het transport als de meest kwetsbare schakel in hun bedrijf. Een groot deel van de gerapporteerde incidenten is inderdaad transportgerelateerd en het gaat hierbij heel vaak om incidenten met grote schades voor de betrokken bedrijven. Sommige experts zien een ontwikkeling waarbij diefstal van handelsgoederen zich heeft verplaatst van de loodsen naar het transport. Volgens hen worden de loodsen in toenemende mate beveiligd en moeilijker te kraken. De dieven zoeken nu de zwakkere schakel op: meestal het transport. Op Schiphol bijvoorbeeld is deze verplaatsing goed te zien. De loodsen van de grote vrachtafhandelaren aldaar waren jarenlang de plaats waar zeer regelmatig grote hoeveelheden goederen verdwenen. Echter, sinds de invoering van de nieuwe Luchtvaartwet in 2003 zijn deze bedrijven gebonden aan strengere veiligheidsmaatregelen en is het aantal diefstallen gedaald. Tegelijkertijd is echter een toename waar te nemen in diefstallen van handelsgoederen bij bedrijven die op de platforms vliegtuigen laden en lossen (dit zijn deels andere bedrijven dan de hiervoor genoemde vrachtafhandelaren). Daar is het proces moeilijker te monitoren en het is duidelijk dat de diefstallen zich verplaatsen van de loodsen naar de platforms (bron KMar).

Daders van interne criminaliteit
Samenvattend kunnen we concluderen dat de gemeenschappelijke kenmerken van interne normovertreders vooral lijken te liggen in het feit dat ze zo weinig gemeenschappelijk hebben. Als we op een rij zetten welke factoren meermalen door respondenten zijn genoemd (let wel: op basis van concrete ervaringen die ze hebben gehad!), dan zien we de volgende 'risicofactoren':

- Werknemers met problemen in de privé-situatie;
- Jonge, laagopgeleide mannelijke werknemers;
- Oudere, hoog opgeleide mannelijke werknemers;
- Allochtone werknemers;
- Autochtone werknemers;
- Werknemers met een slecht ontwikkeld normbesef;
- Werknemers met een te groot uitgavenpatroon (ten opzichte van hun reguliere inkomsten);
- Roekeloze jongeren;
- Werknemers met criminele antecedenten en/of criminele contacten;
- Uitzendkrachten;

[40] De laatstgenoemde factor, aanwezigheid van extern personeel in het bedrijf, is net niet statistisch significant (p=.06).

- Tijdelijke werknemers;
- Werknemers die kort in dienst zijn;
- Werknemers die lang in dienst zijn;
- Werknemers op hun laatste werkdag;
- Werknemers in uitvoerende functies (op de werkvloer);
- Werknemers in controlerende functies (op de werkvloer);
- Werknemers in specialistische of managementfuncties;
- Werknemers die ontevreden zijn;
- Ex-werknemers (die ontevreden waren).

Behalve bij enkele heel specifieke normovertredingen is geen patroon te vinden in de kenmerken van de betrokken normovertreders anders dan dat ze gebruik hebben gemaakt van de 'geboden' gelegenheid. We kunnen ons dan ook aansluiten bij de vaststelling van sommige respondenten en collega-onderzoekers dat het niet zinvol is om een risicoprofiel van de interne normovertreder te maken. Daarvoor is het beeld te diffuus. Bovenstaande bevindingen lijken te bevestigen dat de gelegenheidsstructuur van groter belang is voor de prevalentie van interne criminaliteit dan de persoonlijke of professionele achtergrond van de normovertreder.
Welke betekenis we in dit verband moeten hechten aan de bevinding dat de meeste verdachten die bekend zijn geworden werknemers zijn in doorgaans lager betaalde functies op de werkvloer of in het transport, is niet helemaal duidelijk. Los van de mogelijke rapportagevertekening die zich hierbij voordoet, kunnen we wel concluderen dat op de werkvloer de meeste incidenten plaatsvinden.

Samenvattend kunnen we concluderen dat interne criminaliteit een complex verschijnsel blijkt wanneer we proberen vat te krijgen op de factoren die ermee verband houden. Op het niveau van de organisatie is het gemakkelijker om relevante kenmerken te vinden dan op het niveau van de individuele daders. Of dit ook betekent dat organisatiefactoren belangrijker zijn, valt niet te zeggen. Onduidelijk is immers welke sociale processen schuil gaan achter bijvoorbeeld de relatie tussen omvang van de onderneming en het niveau van interne criminaliteit. Geringere binding van werknemers? Meer tegenculturen? Meer gelegenheid? En hoe moeten we de relatie tussen personeelsproblematiek en interne criminaliteit precies duiden? Mogelijk variëren de antwoorden op deze vragen ook voor verschillende vormen van interne criminaliteit (Giacalone en Greenberg, 1997). Een extra moeilijkheid bij het beantwoorden van dit soort vragen is dat bedrijven niet bij alle interne normovertredingen in gelijke mate zicht hebben op wat zich afspeelt. Dit betekent dat bedrijven die de meeste incidenten rapporteren niet noodzakelijkerwijs ook de bedrijven zijn met de meeste problemen.

5 Preventieve maatregelen en de reactie op incidenten

In dit hoofdstuk behandelen we de onderzoeksvragen 5 tot en met 7.

- *Welke preventieve maatregelen hebben bedrijven getroffen om zich te beschermen tegen verschillende vormen van interne criminaliteit?*
- *In hoeverre leiden veronderstelde of geconstateerde voorvallen van interne criminaliteit tot aanpassingen in het preventiebeleid? Welke obstakels doen zich hierbij mogelijk voor?*
- *Welke (interne en externe) acties ondernemen bedrijven wanneer zij kennis nemen van vermeende of geconstateerde voorvallen van interne criminaliteit? In hoeverre bewandelen zij hierbij strafrechtelijke en/of civielrechtelijke wegen*?

De logistiek dienstverleners in onze steekproef proberen zich al op allerlei manieren en om allerlei redenen te beschermen tegen de in hoofdstuk 3 genoemde gevallen van criminaliteit. Dit doen zij omdat zij bepaalde risico's ervaren die deels zijn gebaseerd op ervaringen in het verleden. Het is daarom belangrijk eerst in paragraaf 5.2 in kaart te brengen welke risico's bedrijven ervaren. In paragraaf 5.3 bespreken wij dan het preventiebeleid van de bedrijven. Enerzijds kijken wij hier naar de mate van beveiliging en factoren die hiermee verband houden. Anderzijds bespreken we mogelijke obstakels bij het realiseren van maatregelen.
Daarnaast hebben wij bij het bespreken van de verschillende normovertredingen gevraagd naar de reactie hierop. In paragraaf 5.4 zijn wij geïnteresseerd in de manier waarop bedrijven zowel intern als extern met incidenten omgaan. Bedrijven kunnen bijvoorbeeld intern hun beveiliging aanpassen na een inbraak en daarnaast extern een particulier recherchebureau inschakelen. Ook kunnen zij ervoor kiezen wel of geen aangifte te doen. In paragraaf 5.5 komt dit aangiftebeleid aan de orde. Bij het nemen van maatregelen en het reageren op incidenten speelt ook de samenwerking met brancheorganisaties, politie en justitie een rol. De tevredenheid over de rol die deze organisaties vervullen, bespreken we in paragraaf 5.6. Het hoofdstuk wordt afgesloten met de conclusies in paragraaf 5.7.

5.1 Meetkwesties

Alvorens over te gaan tot de beschrijving van de onderzoeksresultaten, lichten we kort enkele zaken toe.

5.1.1 Meting van het beveiligingsniveau en de reactie op incidenten

Om een beeld te krijgen van de mate van beveiliging van de verschillende bedrijven hebben wij met onze respondenten een checklist doorgenomen met 26 verschillende preventieve maatregelen en 18 verschillende manieren om bedrijfsprocessen te monitoren (zie bijlage 1, blok 3). Dit laatste is belangrijk omdat op deze manier de goederenstromen en bedrijfsprocessen beter in de gaten kunnen worden gehouden en incidenten eerder aan het licht komen. Vervolgens hebben wij de bedrijven ingedeeld in drie groepen afhankelijk van het totaal aantal beveiligingsmaatregelen (preventie en monitoring opgeteld): laag beveiligde bedrijven (12%, tot 24 maatregelen), middelmatig beveiligde bedrijven (71%, 25-36 maatregelen) en hoog beveiligde bedrijven (18%, 37 of meer maatregelen). Met behulp van deze indeling is het mogelijk de invloed van verschillende variabelen te relateren aan het beveiligingsniveau van bedrijven.
Om in kaart te brengen hoe bedrijven op incidenten reageren, hebben wij bij het bespreken van de laatst voorgevallen individuele normovertredingen ook gevraagd naar de reactie van bedrijven hierop (zie bijlage 2). Daarbij maken wij onderscheid tussen (interne) maatregelen die binnen het bedrijf worden genomen en (externe) reacties waarbij de hulp van buitenaf wordt ingeroepen. Ten slotte hebben wij bij het bespreken van de normovertredingen gevraagd op welke manier bedrijven omgaan met de daders van afzonderlijke vormen van interne criminaliteit.

5.1.2 Overige meetkwesties

Bij de verschillende preventiemaatregelen die wij hebben voorgelegd, zijn verschillende gradaties in het beveiligingsniveau mogelijk die niet naar voren komen uit onze vragenlijst. Een bedrijf kan in de categorie 'camerabewaking binnen' bijvoorbeeld alleen de toegangsdeur van de loods met een camera bewaken of het gehele proces in de loods met digitale beweegbare camera's in de gaten houden. In beide gevallen zal de categorie 'toezichtcamera's binnen' zijn gescoord.
Respondenten kunnen de mate van beveiliging ook bewust of onbewust soms rooskleuriger doen vóórkomen dan deze in werkelijkheid is. Een respondent kan, bijvoorbeeld door een beperkt zicht op alle mogelijkheden om het bedrijf te beschermen, het idee hebben dat zijn bedrijf goed is beveiligd, terwijl wij als onderzoekers bij andere bedrijven veel verdergaande preventieve maatregelen aantroffen. Daarnaast kunnen respondenten onwillig staan tegenover het melden van de zwakke plekken binnen het bedrijf. Een van de contactpersonen die niet wilde meewerken zei ons bijvoorbeeld 'nog niet aan zijn moeder te zullen vertellen waar de zwakke plekken in het bedrijf liggen'. De garantie dat alle informatie vertrouwelijk zou worden behandeld, zal voor sommige respondenten dus niet voldoende zijn geweest. Niemand hangt graag de vuile was buiten. Om enige vertekening in de resultaten tegen te gaan hebben wij achteraf bedrijven beoordeeld op ons idee over de mate van beveiliging. Zoals in hoofdstuk 3 al naar voren is gekomen, hadden wij bij een kleine groep respondenten het idee dat respondenten de mate van beveiliging beter voorstelden dan deze was.
In het geval een bedrijf over verschillende vestigingen beschikt, zullen deze ook niet altijd even goed beveiligd zijn. Dit kan zelfs gelden voor verschillende loodsen op dezelfde locatie. Een nieuw gebouwde loods zal over het algemeen goed zijn beveiligd, terwijl in verouderde loodsen soms nog allerlei verouderde systemen en donkere hoeken zitten die de mogelijkheden voor effectieve criminaliteitspreventie beperken.
Dat respondenten niet altijd over evenveel kennis beschikken, blijkt uit het feit dat sommige respondenten tijdens de interviews aantekeningen maakten over ideeën die zij aan de hand van onze vragenlijst opdeden. Daarnaast zijn niet alle respondenten altijd even goed op de hoogte van de afhandeling van incidenten en het wel of niet nemen van bepaalde maatregelen (dit geldt bijvoorbeeld wanneer een incident zich heeft voorgedaan op een andere dan de eigen vestiging of wanneer de screening van nieuwe personeelsleden valt onder de verantwoordelijkheid van personeelszaken).
Een bijkomend probleem bij de afhandeling van incidenten is het feit dat het lastig is het beveiligingsniveau van een bedrijf te relateren aan het aantal incidenten. Dit komt omdat wij slechts zicht hebben op het huidige niveau van beveiliging, terwijl een incident gebeurde op het moment dat het beveiligingsniveau mogelijk op een lager niveau lag. Wij kiezen dan ook ervoor om de reactie op incidenten te relateren aan allerlei andere variabelen. Gezien het soms lage aantal gerapporteerde incidenten bij bepaalde normovertredingen, zullen wij er daarnaast voor kiezen slechts de reactie op die interne normovertredingen te bespreken, die vaker dan tien keer zijn gerapporteerd.

Concluderend kunnen we zeggen dat in enkele gevallen mogelijk sprake is van overschatting van het aantal genomen maatregelen. Desondanks zal het totaal aantal genomen maatregelen een behoorlijk goed beeld geven van de mate van beveiliging van een bedrijf. Als het gaat om de reactie op incidenten, dan zal incidenteel mogelijk sprake zijn van een onderschatting van de reacties wanneer de respondent geen volledig beeld had. Ook dit levert weinig problemen op voor onze conclusies.

5.2 Risico's die bedrijven ervaren

Om inzicht te krijgen in de redenen van bedrijven om preventiemaatregelen te nemen tegen interne criminaliteit en in te schatten hoe groot het risicobewustzijn van bedrijven is, hebben wij gevraagd voor een aantal aspecten aan te geven in hoeverre bedrijven hier risico's ervaren. Deze risico's zijn meestal gebaseerd op eigen ervaringen en/of eigen inzicht in de mogelijk zwakke plekken binnen het bedrijf.

Risico's binnen het bedrijf

Van de bedrijven in de steekproef geeft 71% aan een bepaalde vorm van interne criminaliteit als risicovol te zien. In bijna alle gevallen noemden respondenten hier een vorm van diefstal. Daarnaast werden hier het doorspelen van bedrijfsinformatie en allerlei soorten schades, waaronder vandalisme, genoemd. Bedrijven in de logistieke dienstverlening met betrekking tot gevaarlijke stoffen gaven verder aan in terrorisme een belangrijke dreiging te zien.[41]
Kijken we naar de doelwitten van interne criminaliteit, dan worden in bijna alle gevallen de handelsgoederen genoemd (tenzij bedrijven werken met laagwaardige goederen). Met name in het geval van geliefde hoogwaardige goederen met een handelbaar formaat (consumentenelektronica, merkkleding, alcoholische dranken, sigaretten, et cetera) zien bedrijven risico's. Daarnaast noemen respondenten europallets, computers op kantoor, dieselolie, rembours- en kasgeld, gevaarlijke stoffen en informatie als belangrijke doelwitten.
Wat betreft de locaties en bedrijfsprocessen menen respondenten in 74% van de gevallen dat een specifieke locatie en in 66% van de gevallen dat een specifiek bedrijfsproces een verhoogd risico op interne criminaliteit met zich brengen. Als locatie noemen bedrijven hier in een zeer groot deel van de gevallen de loods of het transportmiddel. In andere gevallen gaat het om in- en uitgangen, nooduitgangen, de parkeerplaats (op of buiten het terrein), de postbus of het kantoor. Het is niet vreemd dat respondenten in het verlengde hiervan transport, laden en lossen, orderpicking en het afgeven van remboursgelden als meest risicovolle onderdelen van de bedrijfsvoering zien. Het blijkt moeilijk om tijdens de overdrachtsmomenten een goed zicht te houden op al het geld, alle goederen en alle personen. Regelmatig geven respondenten in dit verband aan te vrezen voor een-tweetjes tussen chauffeurs en loodspersoneel. Hetzelfde geldt voor het transport dat, wel of niet uitbesteed, grotendeels buiten het zicht van het bedrijf plaatsvindt. Internationaal transport (buiten de Benelux) lijkt daarbij nog extra risico's met zich te brengen. Andere bedrijfsprocessen die (in veel mindere mate) als risicovol worden ervaren, zijn de automatisering, financiële administratie, planning, retournames, fysieke controles en het inbouwen van apparatuur.
Als het gaat om de meest risicovolle tijdstippen, geeft slechts een kleine meerderheid van de bedrijven (58%) aan op bepaalde momenten extra risico's te ervaren. Meestal is dit in het weekend en 's nachts. Daarnaast noemen zij de decembermaand en de piekmomenten in de seizoenen (voor kleding zijn dat bijvoorbeeld het voorjaar en het najaar wanneer de nieuwe collecties binnenkomen). Tijdens de piekperiodes worden veel bedrijven gedwongen om soms grote aantallen uitzendkrachten in te zetten, die vaak minder goed worden gescreend dan vast personeel. Gezien het grote aantal bedrijven dat hierover begint, worden uitzendkrachten zeer zeker als extra risicovol ervaren. In hoofdstuk 4 wordt hiervoor echter weinig bewijs gevonden; er blijken zelfs helemaal geen specifieke daderkenmerken voor plegers van interne criminaliteit te bestaan. Belangrijker is dan ook mogelijk het feit dat, wanneer meer goederen worden op- en overgeslagen en zich meer mensen in de loods bevinden, het lastiger is een goed zicht te houden op alle processen. Een enkele respondent noemt ten slotte de zomer. Niet alleen zijn er dan vaak vakantiewerkers aanwezig, maar ook worden dan in verband met de warmte de dokdeuren van de loods niet altijd gesloten.
Het aantal incidenten waarmee een bedrijf wordt geconfronteerd is van invloed op de risico's die worden ervaren. Zo hebben bedrijven doorgaans weinig aandacht voor bijvoorbeeld frauderisico's, totdat ze worden geconfronteerd met een concreet incident met een grote schade. Vanaf dat moment wordt pas goed gekeken naar de risico's en de mogelijkheden om deze te beperken. Hoe meer een bedrijf met incidenten wordt geconfronteerd, hoe hoger de ingeschatte risico's. Deze relatie is nog sterker als ook externe vormen van criminaliteit worden meegenomen. Dit wordt bevestigd door Van Dijk et al. (1999: 99) die aangeven dat grote schades als gevolg van (interne) criminaliteit zullen leiden tot meer aandacht voor de mate van beveiliging. Bedrijven die minder risico's ervaren zullen ook minder preventieve maatregelen nemen. Dit kan grotendeels worden verklaard uit het feit dat het hier relatief vaak gaat om kleinere bedrijven met minder risicovolle goederen. Echter, bij dit soort bedrijven is soms ook sprake van naïviteit. Zo zei een respondent: 'Ik ben teveel van goed vertrouwen geweest en ben nu door schade en schande wijs geworden. Er schortte veel aan de beveiliging en ik had niet zomaar al mijn personeel moeten vertrouwen'. Dit beeld kunnen wij als onderzoekers zeer zeker bevestigen (zie ook paragrafen 4.2 en 4.3).

[41] Dit is echter veel meer een extern risico. Desondanks gaven deze bedrijven aan hier veel mee bezig te zijn. Soms benadrukten zij ook de hoop te hebben gehad dat ons onderzoek zich meer op dit thema had gericht.

Risico's van vergelijkbare bedrijven
Tot slot hebben wij de respondenten gevraagd aan te geven in hoeverre zij menen dat bedrijven die in dezelfde branche opereren dezelfde risico's ervaren. Van hen gaf 69% hierbij aan dat andere bedrijven dezelfde risico's lopen. Veelal zijn respondenten van mening dat bedrijven met dezelfde omvang, organisatiestructuur, mate van beveiliging, ligging en soorten goederen dezelfde risico's ervaren. Dit weten zij ook uit de contacten met brancheorganisaties collega's en concurrenten. Opvallend is dat slechts 4 van de 139 respondenten (3%) aangeven te menen dat het eigen bedrijf meer risico's loopt. In alle overige gevallen geven respondenten aan dat het eigen bedrijf bijvoorbeeld beter is beveiligd, betere controles heeft ingebouwd, minder met uitzendkrachten werkt of minder met hoogwaardige goederen in aanraking komt.

Samenvattend kunnen wij zeggen dat grotere en beter beveiligde bedrijven over het algemeen een beter beeld hebben van de mogelijke risico's die zij lopen. De gevaren van fraude of corruptie ziet echter geen van de bedrijven. Zij zien vooral risico's in de diefstal van handelsgoederen. Tijdens het transport en op de overdrachtsmomenten in of om de loods, is het lastig alle geld-, goederen- en personenstromen in de gaten te houden. De aanwezigheid van uitzendkrachten wordt hier steevast als een van de grootste risicofactoren ervaren. Zoals blijkt uit hoofdstuk 4, strookt dit beeld echter niet geheel met de werkelijkheid. De risico's die bedrijven ervaren zijn dan ook niet uitsluitend gebaseerd op ervaringen in het verleden, maar ook op stereotyperingen. Soms zijn bedrijven hierin ronduit naïef. Opvallend is ten slotte dat bedrijven zelden erkennen dat het eigen bedrijf meer risico's loopt dan een ander.

5.3 Preventiebeleid

De risico's die bedrijven ervaren zijn van invloed op de beveiligingsmaatregelen die bedrijven nemen. Om het preventiebeleid van de logistiek dienstverleners in kaart te brengen, bespreken wij achtereenvolgens de mate van beveiliging, de factoren die hierop van invloed zijn en de obstakels die bedrijven ervaren bij het nemen van maatregelen.

5.3.1 Algemeen beeld van de mate van beveiliging

Preventieve maatregelen
Gemiddeld nemen bedrijven 18 van de 26 genoemde preventieve maatregelen. Sommige maatregelen worden door vrijwel alle bedrijven genomen. Zo geldt voor bijna alle bedrijven dat zij 's nachts extern zijn verlicht, dat ze duidelijke afsluitprocedures hebben en een alarminstallatie die in verbinding staat met een meldkamer (zie tabel 9). Ook menen bijna alle bedrijven hun digitale gegevens adequaat te hebben beveiligd tegen zowel interne als externe gevaren. Desondanks geven sommige experts in de sector aan computercriminaliteit als een van de grootste toekomstige bedreigingen voor de logistieke sector te beschouwen. Op het moment dat een criminele bende via een computerinbraak toegang weet te krijgen tot de planning en een overzicht van de goederenstromen, weten zij precies waar en wanneer ze moeten toeslaan.
Veel minder vaak treft men personele beveiliging op het bedrijfsterrein aan.Bijna de helft van de bedrijven (49%) geeft aan dit te hebben, maar dit cijfer is nog een ruime overschatting, omdat sommige bedrijven hierbij ook de surveillance als personele beveiliging hebben aangemerkt. Slechts een minderheid van de door ons bezochte bedrijven maakt daadwerkelijk gebruik van altijd aanwezige persoonlijke bewaking, bijvoorbeeld bij de toegang tot het bedrijf. Ook voor de hand liggende maatregelen als toezichtcamera's buiten (56%) en binnen (58%), versterkte ramen en deuren (59%) en een goede screening van werknemers (56%) worden relatief minder vaak genoemd. Maatregelen die relatief nog minder worden aangetroffen zijn een training voor werknemers in het herkennen van verdacht gedrag (27%), een visitatieregeling voor het fouilleren van personeel (35%) en obstakels tegen ramkraken (36%). Het feit dat slechts een marginale meerderheid (54%) van de bedrijven fraudebeleid als integraal onderdeel van het ondernemingsbeleid aanmerkt en dat er slechts bij 55%

van de bedrijven vastgelegde procedures zijn om fraude te voorkomen, laat zien dat veel bedrijven de risico's van interne en externe criminaliteit inderdaad niet altijd even hoog inschatten.[42]
Bijna de helft van de bedrijven geeft aan hiernaast nog andere maatregelen te nemen. Vaak worden hier maatregelen voor het beveiligen van het transport genoemd (zoals het uitrusten van vrachtwagens met satellietontvangers, king-pin sloten[43] en alarminstallaties). Ook worden bij sommige bedrijven steekproefsgewijs vrachtwagens gevisiteerd, worden loodjes gebruikt om de lading te verzegelen en zijn huiftrailers vervangen door trailers met gesloten opbouw.[44] Daarnaast komen we hier verschillende keren maatregelen tegen als detectie door middel van sensoren (bijvoorbeeld infrarood), detectiepoortjes, hekwerken onder stroom en sociale controle.

Tabel 9 Getroffen preventiemaatregelen (n=139, tenzij anders vermeld)

	% Bedrijven dat maatregel treft
Minimaal wekelijkse back-ups computerbestanden	100%
Interne beveiliging computernetwerk	99%
Terrein/gebouw 's nachts extern verlicht	98%
Externe beveiliging computernetwerk (n=138)	97%
Duidelijke afsluitprocedures	96%
Alarmsysteem in verbinding met meldkamer	95%
Systematisch controleren van (bedrijfs)procedures	89%
Hekwerken/poorten	86%
Duidelijkheid over gevolgen normovertreding (n=138)	86%
Duidelijke functiescheiding	86%
Terrein vrij van opklimmogelijkheden (n=137)	75%
Waardevolle zaken extra beveiligd (n=138)	73%
Toegangscontrole terrein/gebouw	70%
Zichtbare waarschuwing beveiliging (n=136)	68%
Gebruik van toegangspasjes	64%
Interne communicatie over incidenten (n=138)	61%
Ramen/deuren extra versterkt (n=138)	59%
Camera's in gebouwen	58%
Camera's op terrein	56%
Screening (criminele) voorgeschiedenis werknemers (n=134)	56%
Vastgelegde procedures om fraude te voorkómen (n=137)	55%
Fraudebeleid is integraal onderdeel van onderneming (n=138)	54%
Personele beveiliging op terrein (n=138)	49%
Obstakels ramkraken	36%
Visitatieregeling voor personeel (n=138)	35%
Training werknemers herkennen verdacht gedrag	27%

Monitoring

[42] Zoals besproken bij de meetkwesties in paragraaf 1, zal hierbij mogelijk in een aantal gevallen nog sprake zijn van een overschatting van het aantal genomen maatregelen. Met name de vragen over de vastgelegde procedures en het fraudebeleid lijken hiervoor extra gevoelig te zijn, omdat deze breder werden geïnterpreteerd dan fraude en soms als maatregelen tegen criminaliteit in het algemeen werden gezien.
[43] King-pin sloten worden gebruikt om te voorkómen dat losstaande trailers zomaar aan een willekeurige trekker kunnen worden gekoppeld.
[44] Bij huiftrailers is de lading met een zeil afgedekt, terwijl bij trailers met een gesloten opbouw gebruik wordt gemaakt van een afsluitbare harde kast.

Als we kijken naar het aantal maatregelen dat bedrijven treffen om de bedrijfsprocessen te monitoren, dan blijkt dat gemiddeld dertien van de achttien maatregelen worden genomen. Een aantal standaard maatregelen wordt door bijna alle bedrijven genomen (zie tabel 10). Zo laat 100% van de bedrijven de jaarrekening jaarlijks door een extern accountant controleren, worden bij 96% van de bedrijven de kostendeclaraties van het eigen personeel gecontroleerd, wordt in 95% van de gevallen de voorraad regelmatig geïnventariseerd en wordt in 91% van de gevallen de in- en uitgaande goederenstroom gecontroleerd. Met welke precisie dit gebeurt, is natuurlijk weer een tweede. Het blijkt voor veel bedrijven onmogelijk de inhoud van elke doos te controleren als er honderden pallets per dag worden vervoerd. De steeds bredere toepassing van methoden voor tracking & tracing (73% van de bedrijven maakt hiervan gebruik) zorgt wel ervoor dat goederen beter kunnen worden gevolgd. Maatregelen die veel minder vaak worden genomen zijn het registreren van criminele incidenten (58%), het inschakelen van beveiligingsexperts voor het maken van een risicoanalyse (53%), het registreren van niet-werknemers op het terrein (45%) en het trainen van kaderfunctionarissen in het herkennen van risicosignalen bij hun medewerkers (28%). Voor de hand liggende activiteiten als het toepassen van compartimentering van bedrijfsruimten waarbij bepaalde werknemers beperkte toegang hebben tot bepaalde plekken binnen het bedrijf (63%), de screening van telefoon, e-mail en internetverkeer (66%) en het actief bespreekbaar maken van kleine normovertredingen (63%) komen bij ongeveer tweederde van de bedrijven voor.

Tabel 10 Monitoring van bedrijfsprocessen (n=139, tenzij anders vermeld)

	% Bedrijven dat maatregel treft
Jaarlijkse externe accountantscontrole (n=138)	100%
Controle kostendeclaraties personeel	96%
Regelmatig fysieke inventarisatie voorraden (n=138)	95%
Fysiek controleren in-/uitgaande goederen	91%
Gebruik van sleutel- en sluitplan	88%
Overzicht van beschadigde goederen	84%
Gebruik warehousemanagementsysteem	83%
Controle van ieders werkzaamheden	78%
Overzicht van zoekgeraakte goederen	74%
Gebruik tracking & tracing voor goederen	73%
Gebruik van schriftelijke gedragscode (n=138)	71%
Screening van telefoon/internet/e-mailverkeer	68%
Toepassing compartimentering bedrijfsruimten	63%
Actief kleine normovertredingen bespreekbaar maken	63%
Overzicht van criminele incidenten (n=138)	58%
Inschakelen beveiligingsexperts voor risicoanalyse (n=137)	53%
Registratie van niet-werknemers op bedrijf	45%
Functionarissen trainen in herkennen verdacht gedrag (n=137)	28%

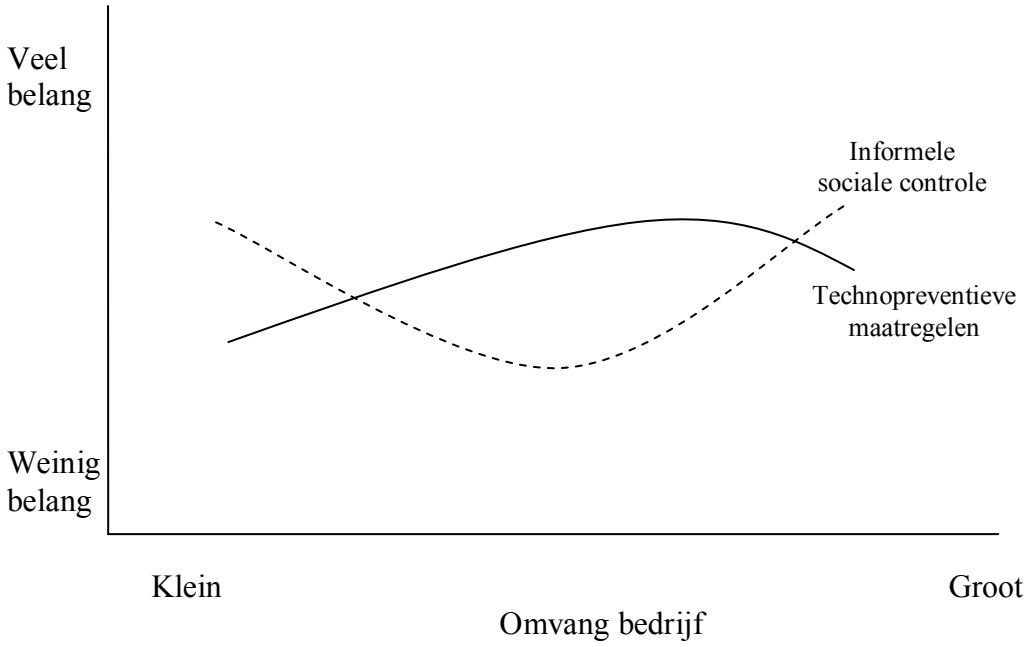
Effectieve maatregelen

In blok 3 van de vragenlijst vragen we ook naar de effectiviteit van al dit soort maatregelen. Respondenten antwoorden in veel gevallen dat maatregelen kostbaar zijn, dat alles wat ze doen nodig is, dat continu verbeteringen noodzakelijk zijn omdat kwaadwillenden inventief zijn en dat de resultaten van de genomen maatregelen moeilijk in te schatten zijn. Het blijkt dan ook lastig in dit verband een goede kosten-batenanalyse te maken.

Wat betreft de (in)effectiviteit van specifieke maatregelen blijken (random) visitatie, cameratoezicht en sociale controle in combinatie met bouwkundige en technologische maatregelen zeer vaak als effectief te worden genoemd. Andere vaker genoemde effectieve maatregelen zijn volgens respondenten het onder stroom zetten van hekwerken, toegangspasjes, compartimentering van bedrijfsruimtes, veiligheidsrondes, communicatie over beveiliging en de noodzaak ervan, en allerlei

beveiligingsmaatregelen om het transport beter te beveiligen. Opvallend is dat bedrijven in dit verband vooral de meest recent genomen maatregelen als effectief beschouwen. Bij de minst beveiligde bedrijven is dit het hekwerk, bij beter beveiligde bedrijven de camerabewaking en bij de best beveiligde bedrijven de visitatie en procedures.
Veel respondenten (in met name de beter beveiligde bedrijven met een hoger risicobewustzijn) zijn het erover eens dat een goede beveiliging van het bedrijf staat of valt met het volgen van procedures. Daar waar procedures niet worden opgevolgd, zal de kans op incidenten enorm toenemen. Bouwtechnische en technologische maatregelen kunnen dit niet ondervangen. Kleine bedrijven met weinig ervaring op het gebied van criminaliteit en criminaliteitspreventie zeggen in dit verband aan sociale controle genoeg te hebben. Naarmate de omvang en het risicobewustzijn van bedrijven groter worden, neemt de kwaliteit van de genomen preventieve maatregelen toe. Aanvankelijk wordt dan vooral geïnvesteerd in bouwkundige maatregelen zoals hekken, daarna meer in technologische maatregelen zoals camerabewaking. De best beveiligde bedrijven met het hoogste risicobewustzijn geven echter aan dat zij toch beperkingen zien in het nemen van oneindig veel bouwkundige en technologische maatregelen. In de literatuur wordt dit bevestigd. De bruikbaarheid van elektronische controlemaatregelen wordt ondermijnd door de mogelijkheid deze te omzeilen en de kans op menselijk falen. Daarnaast wordt slechts de gelegenheid voor interne criminaliteit beperkt en niet de oorzaak hiervan aangepakt (Krause, 2002: 40).
Verschillende experts uit de riskconsultancy- en de verzekeringswereld wijzen daarom consequent erop dat communicatie, sociale controle en het opvolgen van procedures van cruciaal belang zijn bij het optimaal beveiligen van het bedrijf. Ook Traub (1996: 250) geeft aan dat het aanbieden van *awareness* programma's en interne communicatie over het probleem de meest effectieve manieren zijn om interne criminaliteit aan te pakken. Bedrijfsprocedures moeten dan ook goed worden gecommuniceerd. Hier ligt echter bij veel bedrijven een zwakke plek. Op het moment dat procedures worden ingevoerd blijken deze nog wel te worden opgevolgd, maar met de tijd blijkt vaak de aandacht te verslappen en nijgt men weer terug naar de oude situatie. Dit komt met name doordat er vaak organisatorische beperkingen zitten aan het nauwgezet volgen van procedures. Sommige bedrijven proberen hun werknemers daarnaast te stimuleren om in gevallen van interne criminaliteit hiervan melding te maken bij het management. Ook dit blijkt een belangrijke preventiemaatregel te kunnen zijn (Traub, 1996: 251). Immers, op de werkvloer weet men precies wat er gebeurt, aldus onze respondent bij Hoffmann Bedrijfsrecherche. Ten slotte is van belang dat het management het goede voorbeeld geeft (Cools, 1994: 106) en ook optreedt tegen kleine normovertredingen (Wielenga, 1992: 34). Duidelijk is steeds weer dat de mens de cruciale factor blijft. Een en ander wordt verduidelijkt in figuur 3 waarin ter illustratie het belang dat bedrijven hechten aan sociale controle en technopreventieve maatregelen wordt afgezet tegen de omvang van bedrijven.

Figuur 3 Het relatieve belang dat bedrijven hechten aan verschillende soorten preventiemaatregelen afgezet tegen de omvang van bedrijven



Een methode om het niveau van de procedures hoog te houden is het systematisch controleren ervan dat door slechts 55% van de respondenten zegt te worden gedaan. Een ander door verschillende experts aangedragen hulpmiddel voor het structureren van de procedures is het instellen van een gedragscode of specifieke bedrijfscode. De EVO (2004: 19-20) beschrijft de functie hiervan als volgt: 'de gedragscode dient het preventiebeleid te ondersteunen, duidelijkheid te verschaffen over de geldende verantwoordelijkheden, sturing te geven aan wat wordt verwacht van de medewerkers, corrigerend te werken op het niet naleven van de regels en betrokkenheid van de medewerkers te stimuleren'. Een gedragscode bestaat uit algemene regels voor werknemers, bijvoorbeeld over arbeidstijden, ziektemelding, internet- en emailgebruik, onkostenvergoeding, omgang met het personeel, omgang met de middelen van de werkgever en zorgvuldige omgang met de tijdregistratie. Belangrijk is dat duidelijk wordt aangegeven wat gebeurt als overtredingen worden begaan. Het fungeert zowel voor werkgever als voor werknemer als handvat en biedt daarnaast ook bij de rechter houvast in het geval van een ontslagprocedure. Zowel de regels als de communicatie daarover moeten glashelder zijn, aldus TLN (2003: 55).
Van de respondenten geeft 71% aan dat door het bedrijf een schriftelijke gedragscode is opgesteld. Dit lijkt echter een overschatting omdat sommige bedrijven alleen een gedragscode voor chauffeurs hebben (het chauffeurshandboek). Andere bedrijven geven aan ook de afspraken in de CAO en in sommige gevallen mondelinge bedrijfsregels als gedragscode te zien. De respons over de effectiviteit en het functioneren van de gedragscode laat zien dat 50% van de bedrijven die erover beschikken meent dat deze goed functioneert. Bij 30% van de bedrijven functioneert het redelijk en in 10% van de bedrijven niet goed. Over het algemeen geven respondenten aan dat bedrijven de gedragscode inderdaad kunnen gebruiken om hun werknemers zonodig te corrigeren. Echter, in veel gevallen blijken werknemers, ondanks daarvoor bij ontvangst te hebben getekend, de inhoud van de gedragscode nauwelijks te kennen. Een aantal bedrijven geeft dan ook aan de gedragsregels mondeling terug te laten komen tijdens werkoverleg.

Ineffectieve maatregelen
Niet alle maatregelen blijken na invoering even effectief. Met name camera's, screening van personeel en visitatie worden door verschillende respondenten als ineffectief beschouwd. Op de problemen rond de screening van nieuw personeel komen wij later nog terug. Wat betreft visitatie weet men te melden dat sommige bedrijven meerdere uitgangen hebben, dat visitatie plaatsvindt op vaststaande momenten en dat met de komst van de mobiele telefoon in een mum van tijd iedereen in het bedrijf weet dat er wordt gevisiteerd. Ook de camera's die door andere respondenten juist als effectief worden beschouwd (zie hiervoor), blijken bij veel bedrijven problemen op te leveren. Ofwel het levert een onwerkbare

situatie op, ofwel camerabeelden mogen niet worden gebruikt als bewijs, ofwel de beelden zijn zo slecht dat erop niks valt te zien. Daarnaast klaagt men over de opvolging van incidenten. Wanneer het alarm afgaat, blijkt in sommige gevallen de beveiligingsorganisatie pas na een half uur aanwezig te zijn. Een kraak is dan in veel gevallen al gezet. Ook komt het voor dat beveiligingsorganisaties gele kaarten uitdelen voor valse meldingen. Wanneer een bedrijf meerdere gele kaarten heeft ontvangen, komen sommige bewakingsdiensten helemaal niet meer, aldus enkele respondenten.

Samenvattend kunnen wij aangeven dat de nadruk bij de beveiliging sterk ligt op diefstal- en inbraakpreventie met betrekking tot de handelsgoederen, zowel in de loods als tijdens het transport (hoewel dit laatste lastiger is te beveiligen). De beveiligingsmaatregelen die men treft liggen vooral op het fysieke vlak en allerhande controlemaatregelen. 'Zachtere' preventiemaatregelen, zoals sociale controle, het personeelsbeleid en het controleren van bedrijfsprocedures op mogelijke kwetsbaarheden, worden minder vaak getroffen. Door de beperkte effectiviteit van bouwkundige en technologische maatregelen, worden deze 'zachtere' maatregelen door verschillende bedrijven echter als onontbeerlijk beschouwd. Technopreventieve maatregelen dienen dan ook vergezeld te gaan met vastomlijnde procedures en sociale controle. Opvallend is verder dat bij het bespreken van de effectiviteit van preventiemaatregelen, zelden of nooit maatregelen worden genoemd om de goederen en geldstromen in de gaten te houden. Maatregelen als ingangscontroles, voorraadcontroles en tracking & tracing zijn erop gericht om het *dark number* beter in beeld te krijgen en komen hierna nog aan de orde.

5.3.2 Verschillen in preventiebeleid tussen bedrijven

Bijna alle bedrijven treffen een reeks van maatregelen om criminaliteit in het algemeen en interne criminaliteit in het bijzonder tegen te gaan. Niet alle bedrijven zijn echter even goed beveiligd. Er zijn tal van factoren aan te wijzen om deze verschillen in beveiligingsniveau te verklaren.

Locatie, omvang en het soort goederen
Van te voren leken met name de volgende drie factoren belangrijk te zijn voor het verklaren van de variatie in genomen preventieve maatregelen: de omvang van het bedrijf, de locatie waar het bedrijf gevestigd is en de soorten goederen die worden op- en overgeslagen. Zoals valt te verwachten hangt het aantal genomen maatregelen inderdaad samen met de omvang van het bedrijf. Grotere bedrijven blijken significant meer preventieve maatregelen te nemen.
Kijken we naar de mate van beveiliging in de verschillende regio's, dan zijn de resultaten opvallend. In de regio Rotterdam worden relatief weinig preventieve maatregelen getroffen (slechts 14% is hoog beveiligd). In Noord-Brabant en Limburg, waar mogelijk veel familiebedrijven zijn gevestigd, ligt het aantal beveiligingsmaatregelen eveneens relatief laag (17% van de bedrijven is hoog beveiligd). Daarentegen ligt het beveiligingsniveau zeker op Schiphol (67% hoog beveiligd), maar ook in de rest van de randstad (50% hoog beveiligd) juist relatief hoog. Voor de rest van Nederland geldt een gevarieerd beeld (33% hoog beveiligd). De lage cijfers voor Rotterdam zijn deels wel te verklaren. Ondanks het feit dat de bedrijven daar wel degelijk vaak met hoogwaardige producten werken, nemen zij veel minder maatregelen vanwege de vaak geringe omvang van de bedrijven.
Ten derde maken wij een onderscheid op basis van product. Preventieve maatregelen dienen beter te zijn al naar gelang met meer hoogwaardige en diefstalgevoelige goederen wordt gewerkt. Het spreekt voor zich dat een bedrijf dat doet in papier en verpakkingen niet dezelfde mate van beveiliging nodig heeft als een bedrijf dat consumentenelektronica opslaat. Bedrijven met de meest risicovolle goederen blijken dan ook significant meer beveiligingsmaatregelen te treffen.

Andere interne factoren
Een ander aspect dat van invloed kan zijn op de beveiligingsmaatregelen die een bedrijf neemt, is de organisatiestructuur van het bedrijf. Daar waar bedrijven beschikken over een speciaal daarvoor aangestelde *security* manager en/of *security* afdeling, zal het veiligheidsbewustzijn over het algemeen groter zijn. Deze indeling hangt echter nauw samen met de omvang van bedrijven. Zoals valt te verwachten hebben bedrijven met een *security* manager en/of een *security* afdeling dan ook een significant hoger beveiligingsniveau dan bedrijven die dit niet hebben.

Daar waar bedrijven meer gebruik maken van uitzendkrachten ervaren zij meer risico's. Het feit dat bedrijven met uitzendkrachten iets meer maatregelen nemen dan bedrijven zonder uitzendkrachten, blijkt na controle voor de omvang van bedrijven, geen significant verband te zijn. Het percentage uitzendkrachten is dan ook niet gerelateerd aan het beveiligingsniveau van bedrijven.
Een bedrijf dat al of niet uitgebreide bewerkingen uitvoert op zijn producten zal meer controles moeten uitoefenen dan een bedrijf dat puur op- en overslaat, omdat producten hier door meer handen gaan en soms op stukniveau worden verwerkt. Het verschil is hier evident. Negen van de tien bedrijven (en dit zijn niet alleen kleine bedrijven met uitsluitend laagwaardige goederen!) waar alleen op- en overslag plaatsvindt, heeft een laag beveiligingsniveau. Bedrijven die zich uitsluitend bezighouden met op- en overslag blijken significant minder maatregelen te nemen om het bedrijf te beveiligen.
Van belang is daarnaast of een bedrijf het transport van de goederen zelf uitvoert of dit geheel of grotendeels heeft uitbesteed. Zoals reeds eerder besproken, wordt het transport vaak als de zwakste schakel in de logistieke keten beschouwd. Het aandeel van het transport in eigen beheer blijkt echter niet significant te correleren met de genomen beveiligingsmaatregelen.
Ten slotte is in dit verband de in hoofdstuk 3 al uitgebreid besproken *dark number* problematiek van belang. Bedrijven die het *dark number* probleem herkennen blijken nauwelijks betere preventiemaatregelen te nemen dan bedrijven die dit niet doen. Wel nemen goed beveiligde bedrijven die erkennen dat er een grijs gebied is, veel vaker maatregelen om het probleem beter in kaart te brengen dan bedrijven die weliswaar het probleem herkennen, maar veel minder goed beveiligd zijn. Toch nemen bijna alle bedrijven wel maatregelen om het grijze gebied beter te controleren. In heel veel van de gevallen noemen respondenten hier allerlei vergaande ingangs- en uitgangscontroles. Daarnaast worden vaak maatregelen genoemd als tracking & tracing, controles van de vrachtbrieven, jaarlijkse inventarisaties, *cycle counts*[45], visitatie en cameratoezicht. Steeds strengere controles zijn nodig om te kunnen onderzoeken waar in de keten iets wel of niet is misgegaan. Hiermee proberen bedrijven te voorkomen dat zij achteraf door opdrachtgevers of verzekeraars aansprakelijk worden gesteld voor schades of vermissingen die niet in het eigen bedrijf zijn veroorzaakt.

Externe factoren
Naast de hiervoor genoemde factoren kunnen ook nog verschillende externe oorzaken worden genoemd die het beveiligingsniveau van een bedrijf kunnen verklaren. Deze zullen wij hier kort bespreken.
Zoals hiervoor al werd aangegeven zijn de bedrijven op Schiphol relatief het best beveiligd. Dit heeft verschillende oorzaken. Ten eerste zijn de goederen die als luchtvracht worden vervoerd relatief hoogwaardig.[46] Veel van de bedrijven op Schiphol zijn dan ook gespecialiseerd in consumentenelektronica. Deze bedrijven zijn zich al lange tijd bewust van de risico's die zij lopen. De beveiligingseisen leggen bedrijven echter niet alleen zichzelf op. Zo heeft het Regionaal Platform Criminaliteitsbeheersing op Schiphol een eigen keurmerk in het leven geroepen om de criminaliteit op en rond de luchthaven tegen te gaan (de uitvoering hiervan ligt bij de brancheorganisatie ACN). Om dit keurmerk te verkrijgen moet aan bepaalde eisen zijn voldaan. Ook de verladers (de opdrachtgevers en vaak ook producenten en eigenaren van de goederen) stellen eisen. Het transport van hoogwaardige goederen vereist nou eenmaal hogere beveiligingsmaatregelen dan het transport van bulkgoederen. De verladers verenigd in TAPA eisen dan ook van hun logistiek dienstverleners dat zij beschikken over een TAPA-certificering. Een groot deel van de bedrijven in Nederland die over een dergelijk certificaat beschikt, heeft (ook) een vestiging op of rond Schiphol. Niet voor niets is de relatie tussen bedrijven die beschikken over een TAPA-certificering en hun beveiligingsniveau zeer significant. Daarnaast speelt voor bedrijven op Schiphol mee dat zij relatief vaak onderdeel zijn van een grotere buitenlandse onderneming. Op Schiphol is zelfs nog maar één familiebedrijf te vinden. Grote internationale ondernemingen leggen hun buitenlandse vestigingen relatief hoge eisen op ten aanzien

[45] *Cycle counting* is een voorraadmethode waarbij op zeer regelmatige basis kleine delen van de voorraad worden geteld. Het voordeel is dat bedrijven niet hoeven worden stilgelegd voor de jaarlijkse voorraadcontrole en dat goederen meerdere keren per jaar worden geteld. Ook leidt dit tot een hogere voorraadbetrouwbaarheid.
[46] Daarnaast wordt per luchtvracht ook bederfelijke waar vervoerd. De door ons bezochte bedrijven op Schiphol hielden zich voor het overgrote deel echter bezig met hoogwaardige goederen.

van de te nemen beveiligingsmaatregelen. Zij hebben immers een naam hoog te houden. Bij deze bedrijven zal het hoge beveiligingsniveau niet zozeer afhangen van ervaringen in het verleden, als wel van de hoge eisen die 'moeder' stelt.
Ook door de wetgever kunnen allerlei maatregelen worden opgelegd. Vooral de Luchtvaartwet stelt hoge eisen aan de beveiligingsniveaus van de bedrijven die betrokken zijn bij het vervoeren van luchtvracht. Sinds kort zijn ook bedrijven in de zeevracht aan meer controles onderhevig. Logistiek dienstverleners in de grote havens die zaken doen met bepaalde landen (waaronder de Verenigde Staten) en zich bevinden aan een kade, moeten voldoen aan de eisen van de ISPS Code.[47] Het beveiligingsniveau in en rond de haven ligt nu nog ver achter op dat op Schiphol. Dit beeld wordt bevestigd door de Zeehavenpolitie in Rotterdam. Op Schiphol worden al jaren veel hogere eisen gesteld. Om in aanmerking te komen voor de ISPS-certificering zullen de bedrijven rond Rotterdam hun beveiligingsniveau dus flink moeten opschalen.
Tot slot stellen ook verzekeraars meer en meer eisen aan de te nemen preventieve maatregelen. Voor sommige bedrijven is het zelfs niet meer mogelijk met een laag beveiligingsniveau aan een betaalbare polis te komen. Verzekeraars specialiseren zich daarbij ook recentelijk steeds meer in allerlei *audits* en *security checks* om bedrijven te wijzen op hun zwakke punten en de mogelijkheden die er zijn om het bedrijf beter te beveiligen.

Samenvattend kunnen we stellen dat bedrijven relatief goed beveiligd zijn, maar dat er een enorme variatie bestaat in de beveiligingsniveaus van de bedrijven. Een veelheid aan factoren blijkt van invloed op de genomen maatregelen. Grotere bedrijven die werken met hoogwaardigere goederen, nemen meer preventieve maatregelen. Ook speelt mee of een bedrijf beschikt over een speciaal daarvoor aangestelde *security* manager. Daarnaast blijkt van belang of bedrijven ook bewerkingen uitvoeren op de goederen. De aanwezigheid van uitzendkrachten, het wel of niet in eigen beheer hebben van het transport en de erkenning van het *dark number* probleem blijken nauwelijks invloed te hebben. Wat dit laatste betreft geldt wel dat goed beveiligde bedrijven die de *dark number* problematiek herkennen, veel meer maatregelen nemen om het grijze gebied in beeld te krijgen. Bij de mate van beveiliging spelen echter ook externe factoren een rol. Wetgeving, verzekeraars en verladers kunnen eisen stellen aan hun logistiek dienstverleners. Al deze factoren samen kunnen de grote verschillen in het beveiligingsniveau tussen Rotterdam en Schiphol verklaren. Deze bedrijven verschillen op een aantal cruciale punten. Op Schiphol bevinden zich veel vestigingen van grote internationale bedrijven die werken met zeer hoogwaardige goederen, gecertificeerd zijn en beschikken over een *security* manager. De externe eisen voor bedrijven op Schiphol zijn al jaren hoog. Wat dat betreft hebben de bedrijven rond Rotterdam nog een lange weg te gaan.

5.3.3 Obstakels bij het nemen van maatregelen

Het nemen van adequate preventieve maatregelen heeft nogal wat voeten in aarde. In totaal gaf 71% van de door ons ondervraagde bedrijven aan hierbij op de een of andere manier obstakels te ondervinden. Niet alleen dient een lastige afweging te worden gemaakt tussen de kosten en baten van de beveiligingsmaatregelen, maar ook heeft het inpassen van maatregelen soms vergaande invloed op de bedrijfsprocessen. Ten slotte lopen bedrijven soms tegen juridische obstakels aan.

Financiële obstakels
Dat bedrijven het lastig vinden een goede kosten-batenanalyse te maken, kwam ook al naar voren bij het bespreken van de effectiviteit van allerhande maatregelen. Bedrijven geven aan dat het bijna onmogelijk is om precies in te schatten wat de maatregelen opleveren.[48] Daarnaast liggen de kosten

[47] De ISPS Code staat voor de International Ship and Port Facility Security Code. Deze bestaat uit een lijst maatregelen om de veiligheid van schepen en havenfaciliteiten te verbeteren.
[48] In dit verband noemen Van Dijk et al. (1999: 124) ook dat 'indien investeringen in preventie feitelijk leiden tot het verschoond blijven van criminaliteitsschade, het denkbaar is dat preventiemaatregelen op een gegeven moment niet meer als de causale factor worden herkend. In geval van een noodzaak tot bezuiniging zullen deze maatregelen dan ook als eerste weer ter discussie staan.'

van vergaande technopreventieve maatregelen vaak zo hoog dat deze volgens sommige respondenten onbetaalbaar zijn en niet opwegen tegen de risico's die zij worden geacht te verkleinen.
Kennis over wat effectieve beveiliging behelst, is vooral bij kleinere bedrijven, niet altijd aanwezig. Hierdoor kan het lastig zijn een goede afweging te maken tussen de verschillende en vaak kostbare methoden van beveiliging. Echter, ook bij grotere bedrijven zal een *security* manager soms in conflict komen met de commerciële belangen van het bedrijf. Dit geldt des te meer op momenten dat het economisch minder gaat. Veel respondenten zien dan ook financiële obstakels en zullen pas na grote incidenten of in geval van extern opgelegde maatregelen hun beveiligingsniveau opschalen. Voor sommige bedrijven is dit echter onbetaalbaar en zij proberen dan ook op verschillende creatieve manieren deze eisen te omzeilen. Van niet werkende toezichtcamera's gaat immers ook een preventieve werking uit. Een ander voorbeeld is het tijdelijk ophangen van geleende toezichtcamera's wanneer de inspectieteams langskomen of het aanstellen van een 'beveiligingsbeambte' bij de poort zonder dat deze over de vereiste papieren beschikt.
Soms spelen er ook belangenconflicten over welke partij de kosten van beveiliging moet betalen. Dit is vooral aan de orde als de opdrachtgevers van de logistiek dienstverleners bepaalde eisen stellen aan de beveiliging van hun producten. Wel geven bedrijven aan dat een hogere mate van beveiliging ook een commerciële meerwaarde heeft. Sommige verladers doen immers alleen zaken met goed beveiligde bedrijven.

Organisatorische belemmeringen
Er blijken regelmatig organisatorische conflicten te zijn tussen de *security* manager (verantwoordelijk voor de beveiliging) en de operationeel manager (verantwoordelijk voor een efficiënte bedrijfsvoering). Uitgebreide toegangscontroles blijken evenals allerlei ingebouwde controlemaatregelen vertragend te werken. Ook heeft het personeel soms problemen met de maatregelen of deinzen bedrijven ervoor terug maatregelen te nemen omdat zij het wederzijds vertrouwen tussen personeel en management niet willen ondermijnen. Dit geldt vooral voor de kleinere familiebedrijven. Ook in grotere bedrijven komt het echter voor dat ondernemingsraden geplande maatregelen bekritiseren of tegenhouden. Het personeel wordt immers beperkt in zijn vrijheid. Zoals we in hoofdstuk 4 al hebben gezien, uit de weerstand hiertegen zich in sommige gevallen zelfs in de vorm van vandalisme.
Ook op een andere manier lopen bedrijven tegen organisatorische beperkingen aan. In die gevallen waar bedrijven bijvoorbeeld een loods of bedrijfsterrein delen, hebben zij vaak minder mogelijkheden om adequate preventieve maatregelen te nemen. Daarnaast hebben bedrijven soms eenvoudigweg niet genoeg plaats om alle vrachtwagens binnen te parkeren. Ook ontbreekt het vaak aan beveiligde parkeerplaatsen onderweg. Ten slotte klagen sommige bedrijven over de verpakking van goederen. Bijvoorbeeld door de supermarktoorlog, gaan fabrikanten ertoe over om steeds meer te bezuinigen op de verpakking van goederen. Het wordt daardoor makkelijker om goederen uit hun grootverpakkingen te halen. Het is de fabrikant die hier bezuinigt, maar de logistiek dienstverlener is aansprakelijk in geval van diefstal. Op Schiphol geldt in principe hetzelfde. Er ontstaat sneller schade en het is duidelijk zichtbaar wat in welke dozen zit. Volgens sommige respondenten zet dit alleen maar aan tot criminaliteit en draait de logistiek dienstverlener hiervoor op.

Juridische obstakels
Bedrijven ondervinden ook juridische beperkingen. Grotendeels hebben deze te maken met privacywetgeving. Zo kunnen bedrijven niet zo maar visiteren, overal camera's ophangen, de e-mail van werknemers controleren en sollicitanten screenen. Het probleem is vaak dat bedrijven niet goed zijn ingelicht over de juridische beperkingen van allerlei maatregelen. Regelmatig spraken geheel verontwaardigde respondenten over het 'onrecht' dat hen was aangedaan. Als werknemers niet zijn ingelicht over bepaalde maatregelen (zoals de aanwezigheid van camera's) mogen deze bijvoorbeeld niet als bewijsmateriaal worden gebruikt bij een rechtszaak. Inderdaad klagen bedrijven dat zij soms alle bewijzen van bijvoorbeeld een diefstal op tape hebben staan, maar dat de rechtbank dan verklaart dat het bewijs onrechtmatig is verkregen. Het ontslag wordt dan teruggedraaid en de werkgever dient schadevergoeding te betalen. Dit geldt bijvoorbeeld ook als alleen de voorbereidingen voor een inbraak of verduistering zijn vastgelegd of als er alleen serieuze verdenkingen tegen een medewerker

zijn. In dat geval is er toch een heterdaad nodig. Een andere optie is het instellen van een onafhankelijk extern onderzoek om na te gaan of de vermoedens kloppen.
Een bedrijf kan daarnaast niet zomaar telefoons afluisteren en de inhoud van e-mail controleren. Ook indien een bedrijf de mogelijkheid wil hebben te visiteren, dan zal het bedrijf dit vast moest leggen in het arbeidscontract en de bedrijfscode. Visitatie betekent echter niet hetzelfde als fouilleren en kan niet zomaar door iedereen worden gedaan. Het kan alleen met instemming van de medewerker. Ook een beveiligingsbeambte heeft geen bevoegdheid om iemand staande te houden. Wel mag deze, zoals iedere burger, een verdachte aanhouden wanneer deze op heterdaad wordt betrapt. Indien de gedragscode bij iedereen bekend is, kan het bedrijf hierop terugvallen bij een eventuele rechtszaak. Ontbreekt deze, dan is ontslag op staande voet juridisch een moeizaam proces.
Ook als het gaat om het screenen van sollicitanten, hebben bedrijven klachten. De 'verklaring omtrent het gedrag' die sollicitanten krijgen van hun gemeente, biedt soms weinig houvast omdat hierin alleen relevante antecedenten zijn aangegeven.[49] Wel geven sommige respondenten aan dat alleen al het vragen om deze verklaring, een deel van het slechte volk buiten de deur houdt. De screening is ook op andere manieren problematisch. In de meeste gevallen (behalve op Schiphol, waar alle medewerkers die beschikken over een Schiphol-pas aan een AIVD-screening[50] worden onderworpen) heeft het bedrijf weinig mogelijkheden de sollicitanten uitgebreid te screenen. Het kostenplaatje en juridische beperkingen spelen hierbij een rol. Ook het bellen van de laatste werkgever levert niet altijd de gewenste informatie omdat deze misschien juist probeert af te komen van de werknemer en daardoor niet geneigd is de waarheid te spreken. Sommige bedrijven pleiten dan ook voor het opstellen van een zwarte lijst met werknemers die zij buiten de deur wensen te houden. Dit is juridisch lastig, maar de laatste tijd komen hiervoor meer mogelijkheden.[51] Daarnaast zullen bedrijven ook alleen die mensen op de lijst zetten, waarvan zij 100% overtuigd zijn dat deze, ook door de rechtbank, als schuldig worden aangemerkt. Het bedrijf loopt anders immers weer het risico een schadevergoeding te moeten betalen wegens gederfde inkomsten, omdat een werknemer achteraf onrechtmatig op de lijst blijkt te hebben gestaan.
Respondenten noemen ten slotte ook de beperkingen die bijvoorbeeld door de gemeente of de brandweer worden opgelegd. Soms worden bedrijven verplicht toegangsdeuren en nooduitgangen geopend te houden, waar zij deze het liefst zouden willen afsluiten. Waar de politie vraagt om betonnen palen tegen ramkraken, wil de brandweer deze vanwege de brandveiligheid juist niet. Gemeenten zijn daarnaast niet altijd even bereid een bedrijf toestemming te verlenen om het bedrijfsterrein af te sluiten van de openbare weg of bomen (opklimmogelijkheden) te laten kappen.

Samenvattend kunnen wij stellen dat bedrijven nogal wat obstakels tegenkomen als het gaat om het verbeteren van hun beveiliging. Deze liggen op het financiële, het organisatorische en het juridische vlak. Ook zijn zij lang niet altijd even goed ingelicht over de (on)mogelijkheden van bedrijfsbeveiliging. Dit leidt ertoe dat geplande maatregelen soms slechts ten dele of zelfs helemaal niet kunnen worden gerealiseerd. In andere gevallen blijken de nieuwe maatregelen niet toereikend en zitten bedrijven met een enorme financiële strop.

5.4 De reactie van bedrijven op individuele normovertredingen

De mate van beveiliging is zoals wij al hebben gezien mede afhankelijk van de confrontatie met incidenten. In sommige gevallen volgen preventiemaatregelen pas wanneer bedrijven tegen omvangrijke schades aanlopen. Het moge duidelijk zijn dat de reactie van bedrijven vaak afhankelijk

[49] Ondanks de slechte naam die de verklaring omtrent het gedrag heeft, is de kwaliteit van deze verklaring de laatste jaren aanzienlijk verbeterd. Een aantal respondenten lijkt zijn oordeel over de verklaring omtrent het gedrag te baseren op de situatie enkele jaren terug. Eventuele sepots worden er echter niet in opgenomen.
[50] AIVD staat voor Algemene Inlichtingen- en Veiligheidsdienst.
[51] Het College Bescherming Persoonsgegevens (CBP) moet hiervoor toestemming verlenen. Dit kan alleen onder strikte voorwaarden op basis van een door de verschillende partijen opgesteld protocol. In de horeca en de detailhandel zijn voor het opstellen van een dergelijke waarschuwingslijst (beperkte) mogelijkheden gecreëerd. Inmiddels wordt ook gewerkt aan een zwarte lijst voor de gehele transportsector (inclusief de luchtvrachtsector).

is van het soort overtreding.[52] Indien een werknemer regelmatig te hoge telefoonkosten declareert zal een bedrijf eerder geneigd zijn dit intern (bijvoorbeeld met een schriftelijke waarschuwing) op te lossen, dan wanneer een werknemer betrokken is bij een inbraak. In deze paragraaf zullen wij daarom eveneens bespreken hoe bedrijven met eventuele daders omgaan.

5.4.1 Interne maatregelen

Intern kunnen bedrijven verschillende acties ondernemen wanneer zij worden geconfronteerd met incidenten. Zo kunnen de beveiliging en de bedrijfsprocedures worden aangepast of kan een intern onderzoek worden ingesteld. In veel gevallen worden bedrijven zich pas bewust van de risico's die zij lopen op het moment dat zij worden geconfronteerd met een geval van interne of externe criminaliteit. Hoe groter de geleden schade, des te ingrijpender doorgaans de maatregelen die worden getroffen. Incidenten met een geringe schade, waarvan geen dader bekend is, worden daarentegen doorgaans als een regulier bedrijfsrisico aangemerkt. Ook als ze vaak vóórkomen. Op verschillende normovertredingen reageren bedrijven dus verschillend.
Zoals al eerder naar voren is gekomen, geven veel respondenten aan dat het opvolgen van vastgelegde procedures cruciaal is bij de beveiliging van hun bedrijf. Inderdaad blijkt bij incidenten vaak dat bepaalde procedures niet goed zijn gevolgd. Over het algemeen zal pas als reactie op een incident worden bekeken of de bedrijfsprocedures en de beveiliging moeten worden aangepast. In het geval dat de dader niet meteen bekend is, maar interne betrokkenheid wel wordt vermoed, zal ook een intern onderzoek kunnen worden ingesteld.

Intern onderzoek
Een intern onderzoek zullen bedrijven instellen bij incidenten als het doorspelen van bedrijfsgegevens, fraude of vervalsing, inbraak en verduistering. Bij inbraak en verduistering deed men dit in ruim de helft van de gevallen. Men zal in deze gevallen eerder een onderzoek starten als het schadebedrag groot is of als er een patroon is te herkennen in de incidenten. Ondanks het beperkte aantal gevallen blijkt daarnaast dat bedrijven sneller een onderzoek instellen wanneer zij met hoogwaardige goederen werken. Zo stellen bedrijven met hoogwaardige goederen in het geval van verduistering in 31 van de 47 gevallen (66%) een intern onderzoek in, terwijl dit bij goederen met een gemiddeld risico in 14 van de 29 gevallen (48%) gebeurt. Dat is niet vreemd omdat bij deze bedrijven meer geld met de incidenten gemoeid is. Hetzelfde geldt voor grote bedrijven. Zij stellen vaker een intern onderzoek in dan kleinere bedrijven.

Aanpassen beveiliging
Het aanpassen van de beveiliging gebeurt in het geval van verduistering minder vaak dan bij inbraak. Dit komt enerzijds omdat bij gevallen van inbraak gemiddeld hogere schades worden ervaren en anderzijds omdat in geval van verduistering vaak een periode verstrijkt tussen het delict en de vermissing. Het is dan lastiger na te gaan wat er precies is gebeurd. In het geval van een inbraak worden de zwakke plekken meteen duidelijk. Voor wat betreft het aanpassen van de beveiliging zien wij geen verband met de omvang van bedrijven. Wel valt hier op dat bedrijven op Schiphol na een geval van verduistering zelden hun beveiliging aanpassen (11%) en dat bedrijven rond Rotterdam dit juist zeer vaak doen (in 70% van de gevallen). Zoals in paragraaf 5.3 al werd aangegeven wordt dit grotendeels verklaard door het feit dat het niveau van de beveiliging op Schiphol al veel hoger ligt dan die rond Rotterdam. Ondanks het feit dat 62% van de bedrijven aangeeft na een inbraak het beveiligingsniveau aan te passen, blijkt de hypothese dat bedrijven vooral reactief hun beveiligingsniveau aanpassen als reactie op incidenten in het geval van inbraak dus voornamelijk voor de minder beveiligde bedrijven te gelden.

Aanpassen procedures

[52] Zo geven verschillende auteurs in het boek van Giacalone en Greenberg (1997) aan dat zulke verschillende normovertredingen als geweld op de werkvloer, diefstal en sabotage ieder hun eigen aanpak vereisen. Steeds benadrukken zij echter dat bedrijven ook de motieven voor interne criminaliteit dienen aan te pakken door de tevredenheid onder werknemers te vergroten en als management het goede voorbeeld te geven.

Ten slotte kunnen bedrijven ook intern hun procedures aanpassen. Dit doet men bijvoorbeeld in gevallen van grove nalatigheid of in gevallen waarbij door het niet volgen van procedures andere normovertredingen mogelijk zijn geworden (zie hoofdstuk 3). Opnieuw geldt hier dat dit vaker gebeurt in geval van inbraak dan in geval van verduistering.

Samenvattend kunnen we stellen dat hoe groter het bedrijf en hoe hoogwaardiger de goederen, des te eerder een bedrijf een intern onderzoek zal instellen. Kleinere en minder goed beveiligde bedrijven zullen juist eerder hun beveiligingsniveau aanpassen. Hieruit kunnen wij concluderen dat kleine bedrijven, meer dan grote, pas maatregelen nemen om hun beveiliging aan te passen wanneer zij daadwerkelijk geconfronteerd worden met een incident. De interne reactie op incidenten is daarnaast in grote mate afhankelijk van het soort incident. In geval van inbraak, verduistering en in mindere mate fraude, zal men geregeld maatregelen nemen. Bij andere normovertredingen doet men dit veel minder.

5.4.2 Externe maatregelen

Als het gaat om externe maatregelen, kan een bedrijf ervoor kiezen aangifte te doen, een extern recherchebureau, een verzekeraar of andere deskundigen in te schakelen, of bijvoorbeeld omwonenden of brancheorganisaties in te lichten. Bij veel incidenten zal men echter ervoor kiezen om deze vooral intern af te handelen. De belangrijkste reden hiervoor is dat bedrijven willen voorkómen dat ze imagoschade oplopen. Alleen wanneer dit nodig is, zullen bedrijven met incidenten naar buiten treden. Het meest voor de hand ligt hierbij het inschakelen van de politie door het doen van aangifte.

Aangifte
In geval van inbraak geeft 93% van de bedrijven aan hiervan aangifte te doen. Het is niet vreemd dat dit minder vaak gebeurt in het geval van verduistering (in 61% van de gevallen). Dit beeld wordt ook bevestigd door verzekeraars en de politie. Bij een claim richting de verzekeraar is het bedrijf immers verplicht om aangifte te doen. Bij een verduistering zal het echter vaak om kleinere hoeveelheden gaan, zal lang niet altijd een verdachte in beeld zijn en weegt het doen van aangifte en het indienen van een claim mogelijk niet op tegen de opbrengst, de imagoschade en de rompslomp eromheen.
Op Schiphol (80%) en in Rotterdam (77%) zeggen de bedrijven echter vaker aangifte te doen van een geval van verduistering dan in de rest van de randstad (62%), Noord-Brabant/Limburg (52%) en de rest van Nederland (50%). Het maakt daarbij weinig uit om wat voor bedrijf het gaat. Wel is het soort goederen van invloed. Van de bedrijven met goederen met een hoog risico doet 71% aangifte tegenover 43% van de bedrijven met goederen met een gemiddeld risico. Vaker dan uit informatie van de opsporingsdiensten kan worden opgemaakt, geven bedrijven dus aan aangifte te doen. Hierbij zal meespelen dat gevallen van verduistering die niet aan politie en verzekering zijn gemeld, mogelijk ook minder tijdens het interview werden gerapporteerd. Angst voor imagoschade kan hierbij een rol hebben gespeeld.
Van de andere normovertredingen wordt relatief heel weinig aangifte gedaan. Alleen bij overvallen (met interne betrokkenheid) en bij illegale handel werd bijna altijd aangifte gedaan. In het geval van geweld op de werkvloer gebeurde dit in 5 van de 15 gevallen. Bij vervalsing deed men in 5 van de 22 gevallen aangifte. Bij alle overige normovertredingen doet men zelden aangifte en kiest men ervoor de problemen intern op te lossen. Dit kan drie dingen beteken. Enerzijds speelt zoals gezegd imagoschade een rol. Bedrijven zullen dan ook vooral bij kleine incidenten liever zelf de problemen op te lossen. Anderzijds kan dit duiden op een gebrek aan vertrouwen in de politie. Hierop komen wij verderop nog terug. Ten slotte kunnen bedrijven ervan afzien aangifte te doen omdat er geen noodzaak is (bijvoorbeeld omdat het ze niks oplevert).

Inschakelen particulier recherchebureau of accountant
Een kwart van de bedrijven geeft aan in geval van inbraak een particulier recherchebureau in de arm te nemen. Volgens Van Dijk et al. (1999: 97) doen zij dit in gevallen van interne fraude en verduistering soms liever dan de politie in te schakelen. Het is niet gek dat dit met name wordt gedaan door de grote bedrijven omdat dit nu eenmaal een kostbare aangelegenheid is. Zij doen dit in 33% van de gevallen. Dit geldt ook voor bedrijven met risicovolle goederen risicovolle goederen. Ruim eenderde van deze

bedrijven (36%) roept in geval van inbraak de hulp in van een particulier recherchebureau. In geval van verduistering doet men dit in veel minder gevallen omdat de schade gemiddeld lager is. Voor wat betreft de andere normovertredingen gaf men alleen in het geval van het doorspelen van bedrijfsgegevens aan naar een particulier recherchebureau te zijn gestapt. Daarnaast roepen bedrijven in sommige gevallen de hulp in van (forensisch) accountants. Het aantal keren dat dit werd gerapporteerd is echter te laag om conclusies te verbinden aan de omstandigheden waaronder bedrijven dit doen.

Inschakelen verzekeringsmaatschappij
Bedrijven schakelen in het geval van incidenten soms ook de verzekering in. Indien goederen ontvreemd of vermist zijn, zal het bedrijf de eigenaar van de goederen inlichten en die zal dan een claim indienen bij de verzekeringsmaatschappij. De complexiteit van de logistieke keten die al eerder aan de orde is gekomen, maakt dit echter tot een ingewikkelde aangelegenheid waarbij verantwoordelijkheden worden afgeschoven. Niet alleen is vaak onduidelijk wat waar is verdwenen, maar ook is vaak onduidelijk wie waarvoor aansprakelijk is of kan worden gesteld. Als bijvoorbeeld bij de afnemer blijkt dat bepaalde goederen ontbreken, dan zal de hele keten moeten worden nagelopen om te ontdekken waar iets is misgegaan. Mocht dit een groot grijs gebied zijn, dan zal er voor het bedrijf dat weet dat het intern is misgegaan, geen enkele stimulans zijn om dit kenbaar te maken. Erkenning dat de fout intern ligt, zal immers leiden tot imagoschade en aansprakelijkheidsstelling. Een bedrijf zal dan ook alles eraan doen om dergelijke zaken intern te houden en geen aangifte te doen bij de politie.
De praktijk is dat bedrijven elkaar en hun eventuele onderaannemers aansprakelijk proberen te stellen. De bedragen die de verzekering uitkeert, liggen immers vaak veel lager dan de werkelijke waarde van de goederen omdat een verzekeringsmaatschappij de goederen slechts tot een bepaald bedrag per kilo vergoedt. De complexiteit van de keten zorgde ervoor dat in het verleden in veel gevallen de verlader gedupeerd werd of dat hij zijn aanvullende goederenverzekering moest aanspreken. Recentelijk zien bedrijven echter meer en meer een claimcultuur ontstaan, waarbij verladers of hun verzekeringsmaatschappijen proberen de logistiek dienstverleners of anderen in de keten aansprakelijk te stellen. De verzekeringsmaatschappij is immers veel eraan gelegen om niet te hoeven uitkeren. In het geval sprake is van een grote schade door verduistering of inbraak, zal een expertisebureau namens de verzekeraar langskomen om te controleren of aan alle eisen voor het vervoer en de opslag van goederen is voldaan.[53] Alleen dan kan een logistiek dienstverlener zich beroepen op overmacht. Al onze bedrijven geven weliswaar aan goed te zijn verzekerd[54], maar dit is alleen zo indien zij alle procedures strikt hebben gevolgd. In die gevallen dat de vervoerder zelf schade veroorzaakt of dit had kunnen voorkomen is hij aansprakelijk. Het gevolg van deze ingewikkelde claimcultuur is dat verzekeringsmaatschappijen steeds hogere eisen gaan stellen aan het beveiligingsniveau van logistiek dienstverleners. Behalve het feit dat steeds hogere premies moeten worden betaald, nemen hierdoor ook de kosten voor het treffen van beveiligingsmaatregelen navenant toe.
Waar door logistiek dienstverleners onderaannemers worden ingeschakeld voor het transport, zullen ook deze transportbedrijven aan alle eisen moeten voldoen (waarbij de vraag kan rijzen wie voor deze maatregelen moet betalen). Hier zijn met name de kleinere transportbedrijven soms de dupe. De marges in het transport zijn immers klein, de beveiliging ervan is problematisch en de risico's zijn groot. In het geval dat kleinere transportbedrijven voor incidenten aansprakelijk worden gesteld, bestaat een gerede kans dat zij over de kop gaan.

Samenvattend kunnen wij stellen dat bedrijven vaker aangifte zeggen te doen dan wij op grond van onze expertinterviews zouden verwachten. Zeker in geval van een inbraak, overval of de handel in illegale goederen, geven bedrijven aan dit vaak te doen. Bij de motieven voor het doen van aangifte bij een inbraak spelen de omvang van de schade, de hoogwaardigheid van de goederen en eisen van verzekeraars een belangrijke rol. In geval van verduistering geldt dit minder. Daarvan wordt door de relatief lagere schade en de afwezigheid van bekende daders veel minder vaak aangifte gedaan. Door

[53] Deze eisen verschillen afhankelijk van het soort goederen dat wordt verwerkt of vervoerd.
[54] Hierbij moet wel vermeld worden dat het eigen risico soms zo hoog is dat dit door kleinere bedrijven nauwelijks kan worden opgebracht.

de complexiteit van de keten is ook vaak onduidelijk bij wie de verantwoordelijkheid voor een vermissing ligt. Om een claim te voorkomen proberen bedrijven dan ook de schuld af dan wel door te schuiven. Verzekeraars en verladers reageren hierop door steeds hogere eisen te stellen en strikt te controleren of procedures wel goed zijn gevolgd. Andere externe maatregelen worden minder genomen. Het inschakelen van een particulier recherchebureau gebeurt met name door de grotere bedrijven met risicovolle goederen.

5.4.3 Reactie op daders

Bedrijven kunnen ook op verschillende manieren omgaan met de dader(s) van incidenten. Naast het doen van aangifte, kunnen zij de dader bijvoorbeeld ontslaan, een schriftelijke of mondelinge waarschuwing geven, of herplaatsen binnen het bedrijf. Ook kan men de identiteit binnen het bedrijf bekend maken of proberen de schade op de dader te verhalen middels een onderlinge regeling of via de straf- of civiele rechter. Als het gaat om het omgaan met verdachten is dit lastig per normovertreding uit te splitsen omdat het dan steeds om weinig gevallen gaat. Alleen als het gaat om inbraak, verduistering en fraude zijn hieraan conclusies te verbinden.

Vrijwillig of gedwongen ontslag
In een grote meerderheid van de gevallen van inbraak, verduistering en fraude gaan bedrijven ertoe over de dader(s) vrijwillig of gedwongen ontslag te laten nemen. Dit gebeurt bijvoorbeeld in 77% van de 53 gevallen dat bij een verduistering de identiteit van een interne werknemer bekend is geworden. Iets vaker gebeurt dit in bedrijven met risicovolle goederen (84%) dan in bedrijven met goederen met een gemiddeld risico (67%). Soms is ontslag echter helemaal niet aan de orde, bijvoorbeeld als het gaat om een externe chauffeur of een ex-medewerker.

Intern oplossingen zoeken
Indien geen aangifte wordt gedaan geven bedrijven vaak een mondelinge of schriftelijke berisping. Ook zijn bedrijven soms bereid géén aangifte te doen of de aangifte in te trekken als een schaderegeling is overeengekomen. Zij zien de dreiging aangifte te doen dan als een middel om een schaderegeling overeen te komen of de werknemer ‘vrijwillig’ ontslag te laten nemen. Bij veel gevallen van interne criminaliteit die door meerdere personen worden gepleegd (bijvoorbeeld het indienen van te hoge kostendeclaraties of overmatig telefoongebruik) kiezen bedrijven ervoor om naar alle werknemers een memo rond te sturen dat hierop streng zal worden gecontroleerd. Daarnaast gaan zij soms een groepsgesprek aan. Sommige respondenten benadrukken dat het noodzakelijk is dit soort problemen bespreekbaar te maken.

Inschakelen civiele of strafrechter
Bedrijven kunnen de civiele rechter of de strafrechter inschakelen om een ontslagprocedure in te zetten of bijvoorbeeld een schadevergoeding te eisen. Opvallend is dat, in de gevallen dat men bij een incident de civiele rechter inschakelt, dit vrijwel altijd wordt gedaan door een groot bedrijf dat werkt met risicovolle goederen. In mindere mate geldt dit ook voor de gang naar het strafrecht. Kennelijk gaan kleinere bedrijven zelden ertoe over om zulke stappen te ondernemen. Bedrijven die wel gerechtelijke stappen ondernemen om te proberen een werknemer te ontslaan, klagen echter over de problemen die zij hierbij ondervinden. Niet alleen is het een kostbaar en tijdrovend traject, maar ook komt het vaak voor dat werkgevers door de civiele rechter worden teruggefloten wegens het aandragen van onrechtmatig of onvoldoende bewijs. Een werknemer was dan bijvoorbeeld niet op de hoogte van het feit dat camera’s waren geplaatst. In zulke gevallen levert dat het bedrijf een enorme schadepost op omdat deze dan niet alleen opdraait voor de kosten van de rechtsgang, maar ook de werknemer nog een flinke afkoopsom moet betalen. In andere gevallen komt de betreffende werknemer gewoon weer in dienst met alle ongewenste gevolgen voor een verstoorde werkrelatie van dien. Aangezien werknemers in een groot deel van de gevallen minimaal gedeeltelijk in het gelijk worden gesteld, proberen veel bedrijven dit traject te vermijden. Slechts een enkele keer krijgt de werkgever volledig gelijk of wordt bijvoorbeeld een schadevergoeding toegewezen.

Concluderend kunnen wij stellen dat bij bepaalde normovertredingen in een zeer groot gedeelte van de gevallen wordt gepoogd om de dader(s) vrijwillig of gedwongen ontslag te laten nemen. Lukt dit niet, dan kiest het bedrijf voor het doen van aangifte. Alleen in het uiterste geval zal het bedrijf nog kiezen voor een civiele rechtszaak of zich voegen in een strafrechtszaak. Gezien de negatieve ervaringen die veel bedrijven hiermee hebben gaat de voorkeur echter niet hiernaar uit. Bij minder gevoelige normovertredingen zullen bedrijven eerder kiezen voor een mondelinge of schriftelijke waarschuwing, het rondsturen van memo's of het aangaan van een groepsgesprek.

5.5 Aangiftebeleid

Zoals hiervoor al is besproken, zullen bedrijven niet in alle gevallen aangifte doen. Op de vraag of bedrijven een algemeen beleid hebben als het gaat om het doen van aangifte, geeft 32% van de bedrijven aan dit altijd te doen, bijvoorbeeld omdat dit een principe kwestie is of omdat zij hiertoe verplicht zijn volgens de Luchtvaartwet of een ondertekend convenant. In slechts 6% van de gevallen geven bedrijven aan nooit aangifte te doen omdat dit toch geen zin heeft. In alle andere gevallen geven bedrijven aan dat het doen van aangifte afhangt van de situatie. Zoals we al hebben gezien spelen de schade, het soort goederen, druk van de verzekeraar en de bekendheid van een dader hierbij een rol. Van verschillende experts kregen wij te horen dat in relatief weinig gevallen aangifte wordt gedaan. Hierdoor zou slechts een deel van de werkelijke omvang van het criminaliteitsprobleem zichtbaar zijn. Zo hoorden wij van de Zeehavenpolitie in Rotterdam dat alleen aangifte van verduistering wordt gedaan als de dader niet op een andere manier kan worden weggewerkt door het bedrijf. Dit beeld is anders dan het beeld dat bedrijven schetsen. Weliswaar zegt slechts 33% van de bedrijven in geval van verduistering altijd aangifte te doen, maar toch geeft bijvoorbeeld 57% van de grote bedrijven aan de laatste drie jaar minimaal regelmatig aangifte te hebben gedaan. Van de bedrijven met een hoog beveiligingsniveau en een *security* manager zegt 48% zelfs altijd aangifte te doen. Slechts een zeer klein aantal kleinere bedrijven geeft aan principieel nooit aangifte te doen.
Het meest opvallende hier is echter dat 73% van de bedrijven op Schiphol aangeeft altijd aangifte te doen, terwijl bedrijven dit landelijk slechts in 36% van de gevallen doen. Dit heeft te maken met het soort goederen, de goede relatie die veel van de bedrijven hebben met de KMar op Schiphol, het hoge beveiligingsniveau van de bedrijven, de aanwezigheid van een *security* manager en de eisen die door ACN en de Luchtvaartwet worden gesteld. Wat verder opvalt, is dat bedrijven in Rotterdam bij de reactie op normovertredingen aangeven in een groot deel van de gevallen aangifte te doen, terwijl zij hiervoor geen algemeen beleid zeggen te hebben. Ook strookt dit niet met de conclusies van de Zeehavenpolitie ter plaatse.
Grote, goed beveiligde bedrijven met een *security* manager blijken heel duidelijk vaker een algemeen beleid te hebben als gaat om het doen van aangifte. Bij andere bedrijven zijn vaker de omstandigheden bepalend. Het soort goederen en de geleden schade zijn hierbij van belang. Soms worden bedrijven ook tot aangifte aangezet door de verzekering of de opdrachtgever, of er is een concrete verdachte bekend die men aan de politie wil overdragen. Het komt dan ook in slechts enkele gevallen voor dat bedrijven zeggen nooit aangifte te doen. Desondanks concluderen wij op basis van gegevens van de opsporingsdiensten dat hier waarschijnlijk sprake is van een niet te verwaarlozen overschatting. In werkelijkheid zullen bedrijven er lang niet altijd toe geneigd zijn om aangifte te doen.

5.6 Oordeel van bedrijven over brancheorganisaties, politie en justitie

Brancheorganisaties en politie hebben een functie bij het nemen van maatregelen en het omgaan met incidenten. Wij vroegen bedrijven daarom om hun ervaringen met deze partijen.

Brancheorganisaties
Het beeld is hier wisselend. Een zeer groot deel van de bedrijven geeft aan op dit gebied heel weinig ervaring te hebben en alle maatregelen op eigen initiatief te nemen. Sommige bedrijven geven aan hier een stuk ondersteuning te missen, terwijl andere de preventie als een eigen verantwoordelijkheid beschouwen. Dit gebrek aan ervaringen zorgt wel ervoor dat verwachtingen over de

brancheorganisaties niet altijd even hoog gespannen zijn. Volgens enkele respondenten doen de brancheorganisaties al met al te weinig om het thema criminaliteit bij overheid en politie aan te kaarten en geven zij te weinig voorlichting over de effectiviteit van preventiemaatregelen en de mogelijkheden van allerlei certificeringen. Informatie komt vaker van een recherchebureau, de verzekeraar, van internet of uit de krant. Deze informatie is soms echter doorspekt met commerciële belangen. Een respondent gaf dan ook aan behoefte te hebben aan onafhankelijke voorlichting vanuit een centraal informatiepunt. In die gevallen waar wel een goed contact bestaat tussen bedrijf en brancheorganisatie is de mening over deze organisaties vaak wel positief. Zo zijn bedrijven op Schiphol te spreken over ACN, zijn TAPA-gecertificeerden tevreden over de ondersteuning door TAPA EMEA en geven ook enkele leden van brancheorganisaties als TLN, EVO en Fenex aan tevreden te zijn over de ondersteuning. 'Als je ervoor open staat, dan hebben zij goede adviezen', zo is de mening van bedrijven.

Politie

Over de politie zijn bedrijven over het algemeen slecht te spreken. De kritiek richt zich hierbij vooral op het doen van aangifte. Deze tijdrovende aangelegenheid levert zelden iets op. Soms moet speciaal een afspraak worden gemaakt, soms kan de aangifte niet elektronisch en soms heeft de politie helemaal geen tijd en komt men niet eens langs voor sporenonderzoek. Komt het bedrijf achteraf met (externe) tips of verdachten naar de politie, dan levert dit voor de politie vaak te weinig concreet bewijs op en trekken zij de aanwijzingen niet eens na, aldus respondenten. Talloos zijn de verhalen over meldingen of aangiften van diefstallen (met soms grote schades) waarvan de bedrijven vervolgens nooit meer iets vernemen. De meeste bedrijven, die ooit aangifte hebben gedaan bij de politie, hebben dan ook geen idee wat er met deze aangiften is gebeurd. Ten slotte bestaat er onduidelijkheid over het doen van aangifte an sich. Het is het niet altijd duidelijk waar (in welke politieregio of zelfs welk land) en door wie (bedrijf, opdrachtgever of slachtoffer in geval van bijvoorbeeld een overval op een vrachtwagen) aangifte moet worden gedaan.

Zoals we hebben gezien doen bedrijven slechts in een deel van de gevallen aangifte. Bedrijven geven aan dat hier sprake is van een belangentegenstelling. Het bedrijf wil zijn goederen terug, de dader ontslaan, geen ruchtbaarheid aan de zaak geven en zo snel mogelijk 'back to business', terwijl de politie vooral is geïnteresseerd in het pakken van de dader(s). Of zoals een respondent het zei: 'het maakt mij niet uit of ze de dader wel of niet oppakken en straffen. Als ik hem maar kwijt ben'. De politie beaamt deze belangentegenstelling, maar zegt hierdoor ook te worden tegengewerkt. Zouden bedrijven vaker aangifte doen, dan zou de politie een veel beter beeld hebben van wat er werkelijk speelt.[55] Nu doen veel bedrijven alleen aangifte als het niet lukt om een werknemer 'vrijwillig' ontslag te laten nemen. De risico's van imagoschade, de tijdrovendheid van het doen van aangifte en het geringe vertrouwen in opsporingsonderzoek en vervolging van de dader(s) zorgen ervoor dat bedrijven weinig stimulans hebben om aangifte te doen. Traub (1996: 248) bevestigt deze tendens. Volgens hem heeft dit er toe geleid dat veel daders van interne criminaliteit slechts worden ontslagen en niet worden gestraft. Zo ontstaat een vicieuze cirkel waarbij de politie steeds minder goed weet wat er speelt en bedrijven steeds minder aangifte doen. Het moge duidelijk zijn dat bedrijven de preventieve werking van sancties onderschatten. Green (1990: 235) en andere auteurs geven immers aan dat interne criminaliteit deels kan worden voorkomen wanneer werknemers vrezen voor financiële sancties, ontslag, negatieve publiciteit en gevangenisstraffen.

Ook op andere punten is er kritiek op de politie. Opvallend is het aantal bedrijven dat een vergelijking maakt met het veiligheidskeurmerk voor particuliere woningen. Voor bedrijven bestaat zoiets niet, terwijl bedrijven juist aangeven behoefte te hebben aan tips over betere beveiliging en voorlichting over mogelijke dreigingen. Bedrijven verwachten ook preventieve actie van de politie, maar worden hierin steeds teleurgesteld. Met name tijdens het laden en lossen in winkelstraten, tijdens het transport en op parkeerplaatsen verwachten zij meer van de politie. Daarnaast is het zeer moeilijk om de vermissing van goederen aan te geven. Sommige bedrijven pleiten voor een centraal punt waar zij de

[55] Ook Van Dijk et al. (1999: 97) bevestigen deze tegenstelling. Aan de ene kant wordt controle- en opsporingsinstanties verweten dat ze te weinig oog hebben voor de belangen van het bedrijfsleven. Aan de andere kant bestaat het verwijt dat het bedrijfsleven geen opening van zaken geeft.

serienummers van vermiste goederen elektronisch kunnen doorgeven. In Duitsland schijnt dat te kunnen.
De frustraties over de politie worden nog eens versterkt door het feit dat bedrijven aangeven tegen teveel regels aan te lopen als het gaat om de maximum snelheid, het maximum gewicht en de rijtijden. 'Ze delen alleen bekeuringen uit en vangen geen boeven'. Op minimale overtredingen staan hoge boetes die niet te verhalen zijn op de chauffeurs. Veel respondenten geven aan dat bedrijfscriminaliteit absoluut geen prioriteit heeft bij de politie. In veel gevallen is de capaciteit onvoldoende. Bedrijven moeten zelf hun problemen maar oplossen en regelmatig geven bedrijven aan zich totaal vogelvrij te voelen. Meerdere keren maakten respondenten tijdens onze interviews deze onvrede ook in woord en gebaar kenbaar.
De meningen over de politie zijn echter ook sterk verdeeld. Waar respondenten bijvoorbeeld politie-ervaring hebben, zijn zij over het algemeen tevreden over de politie. Over de Waterpolitie en de Zeehavenpolitie komen ook enkele keren positieve geluiden naar voren. Op Schiphol geeft een aantal bedrijven aan goede contacten te hebben met de Koninklijke Marechaussee, ondanks het feit dat daar vanwege de prioriteit voor de bolletjesslikkers, sprake is van een duidelijke onderbezetting. Communicatie over het probleem en getoonde betrokkenheid blijken dus voor veel bedrijven al heel belangrijk als het gaat om het vertrouwen dat zij in de politie stellen. Ook in de Monitor Bedrijven en Instellingen (NIPO, 2002: 64) wordt deze conclusie bevestigd: een snelle en correcte afhandeling van aangiften, probleemoplossend vermogen en kennis van zaken bepalen de mate van tevredenheid over de politie.

Justitie
Ook op justitie wordt kritiek geuit, al weten bedrijven vaak niet wat met een aangifte is gebeurd. Het enige wat zij dan weten, is dat de dader niet is veroordeeld. Waar verdachten wel worden veroordeeld, staan de straffen volgens deze respondenten niet in verhouding tot de bedragen die met de incidenten zijn gemoeid. Voor een enorme kraak komen veel daders er vanaf met een taakstraf of in een enkel geval met een korte vrijheidsstraf. Sommige respondenten noemen deze vorm van criminaliteit dan ook veel lucratiever en minder risicovol, dan bijvoorbeeld de drugshandel.
Voor verschillende respondenten is de onvrede over het *straf*rechtelijke traject gekoppeld aan hun ervaringen in het *civiel*rechtelijke traject. Vooral bij ontslagprocedures tegen bijvoorbeeld een stelende werknemer worden bedrijven achteraf regelmatig door de rechter in het ongelijk gesteld. Volgens deze rechter staat dan bijvoorbeeld het ontslag niet in verhouding tot het delict. Het bedrijf wil echter ook af van werknemers die betrapt zijn op verduisteringen van kleine omvang.

Samenvattend kunnen we stellen dat bedrijven veel klachten hebben over de politie en in mindere mate over justitie en de brancheorganisaties. Communicatie speelt een belangrijke rol bij de totstandkoming van dit oordeel: bedrijven die het gevoel hebben dat ze gehoord worden, zijn doorgaans positiever gestemd over de hiervoor genoemde partijen.

5.7 Samenvatting en conclusie

In dit hoofdstuk hebben wij een beeld gegeven van de preventieve maatregelen die bedrijven nemen en de manier waarop zij reageren op incidenten. Beveiligingsmaatregelen worden genomen op basis van de risico's die bedrijven ervaren, de incidenten waarmee zij geconfronteerd worden en extern opgelegde eisen. Met name in diefstal van handelsgoederen zien bedrijven een groot risico. Tijdens de overdrachtsmomenten blijkt het een zware opgave om alle geld- en goederenstromen, alsmede de personen die hierbij zijn betrokken, in de gaten te houden. Het transport wordt hierbij als het meest risicovol ervaren, gevolgd door de activiteiten in de loods. De risico's die bedrijven zeggen te lopen, zijn behalve op eigen ervaringen, ook op vooroordelen gebaseerd. In fraude en corruptie zien bedrijven veel minder gevaren.
De beveiligingsmaatregelen die men mede op basis van deze risico's neemt, liggen vooral op het fysieke vlak en worden aangevuld met allerlei controlemaatregelen. De minst beveiligde bedrijven waar sociale controle nog hoog in het vaandel staat, zullen eerst bouwkundige maatregelen nemen. Gemiddeld beveiligde bedrijven zullen vervolgens technologische middelen inzetten om hun bedrijf

beter te beschermen. De best beveiligde bedrijven geven vooral aandacht aan de procedures en vallen ten slotte ten dele weer terug op sociale controle. Dit wordt verklaard door de beperkte effectiviteit van bouwkundige en technologische maatregelen. De uiteindelijke beveiliging van een bedrijf valt of staat met sociale controle en het opvolgen van procedures.
Inderdaad komen bedrijven nogal wat obstakels tegen als het gaat om het verbeteren van hun beveiliging. Deze liggen vooral op het financiële, het organisatorische en het juridische vlak. Financieel is lastig in te schatten wat beveiligingsmaatregelen zullen opleveren. Criminaliteit is immers nooit geheel uit te bannen. Daarbij komt dat de kennis van bedrijven soms ontoereikend is om een goede afweging tussen alle mogelijke maatregelen te maken. Ook organisatorisch lopen bedrijven tegen verschillende obstakels op. Preventieve maatregelen werken immers vaak vertragend op het bedrijfsproces. Ten slotte noemen bedrijven diverse juridische belemmeringen die vooral verband houden met privacywetgeving.
De reactie op incidenten verschilt van bedrijf tot bedrijf. Hoe groter de bedrijven en hoe hoogwaardiger de goederen, des te eerder zullen bedrijven een intern onderzoek instellen wanneer zij worden geconfronteerd met een geval van interne criminaliteit. Kleinere bedrijven zullen juist eerder hun beveiligingsniveau aanpassen. Het zijn vooral deze kleinere bedrijven die hun beveiligingsniveau pas zullen opschalen na geconfronteerd te zijn met een omvangrijke schade. In geval van inbraak, verduistering en in mindere mate fraude, zal men in veel gevallen interne maatregelen nemen. Bij andere normovertredingen doet men dit veel minder.
Kijken we naar de externe reactie van bedrijven, dan zeggen zij vaker aangifte te doen dan uit de informatie van opsporingsinstanties mag worden verwacht. Kennelijk hebben bedrijven redenen om niet te melden dat zij incidenten soms liever intern afhandelen. Bij grote incidenten zoals inbraak, doen zij vaker aangifte dan bij verduistering. De schade en het soort goederen spelen hierbij een belangrijke rol, alsmede de verplichting tot het doen van aangifte die door bijvoorbeeld verzekeraars wordt opgelegd. In die gevallen en bij die normovertredingen die men liever intern houdt of waarbij de schade minder groot is, doen bedrijven veel minder vaak aangifte. Grote, goed beveiligde bedrijven met een *security* manager blijken in dit verband vaker het beleid te hebben om wel aangifte te doen. Bij veel andere bedrijven hangt de reactie af van individuele factoren.
Bedrijven geven aan het belangrijk te vinden van de daders van interne criminaliteit af te komen. Zeker in geval van grote schades waarbij de dader bekend is geworden, zal een bedrijf veel eraan zijn gelegen de werknemer te ontslaan. De keuze voor het doen van aangifte zal dan ook deels gebaseerd zijn op de (on)mogelijkheid de dader op andere manieren kwijt te raken. De stap naar de civiele rechter wordt alleen in het uiterste geval genomen. Gezien de negatieve ervaringen die veel bedrijven hiermee hebben gaat de voorkeur echter niet hiernaar uit. Bij minder gevoelige normovertredingen zullen bedrijven eerder kiezen voor een mondelinge of schriftelijke waarschuwing, het rondsturen van memo's of het aangaan van een groepsgesprek.
Andere externe maatregelen worden minder vaak genomen. Alleen grote bedrijven die werken met risicovolle goederen beschikken over de financiële middelen om een particulier recherchebureau in te schakelen. Wel is er veel contact met de verzekeraars. Door de complexiteit van de keten is vaak onduidelijk bij wie de verantwoordelijkheid voor een vermissing ligt. Om een claim te voorkomen proberen bedrijven de schuld af te schuiven. Verzekeraars en verladers reageren hierop door steeds hogere eisen te stellen en strikt te controleren of procedures wel goed zijn gevolgd.
Als het gaat om het beveiligen van het bedrijf en het reageren op incidenten, hebben bedrijven behoefte aan een goede communicatie met de brancheorganisaties en met name de politie. Veel bedrijven voelen zich nu vogelvrij verklaard, omdat zij het gevoel hebben meer te worden tegengewerkt, dan te worden ondersteund in hun strijd tegen criminaliteit. Zij hebben het idee dat burgers altijd voorrang krijgen boven bedrijven. Met name rond het doen van aangifte zijn er veel klachten, maar ook op andere gebieden willen bedrijven verbeteringen. Van cruciaal belang zijn goede contacten, een bereidwilligheid te luisteren naar bedrijven, betrokkenheid bij het nemen van maatregelen en een snelle afhandeling van aangiften. Echter, ook de bedrijven zelf kunnen nog veel doen als het gaat om het nemen van betere preventiemaatregelen. Zij maken zelden gebruik van alle mogelijkheden die er zijn. Ook minder kostbare maatregelen, zoals een goede screening van nieuw personeel en het opzetten van en vasthouden aan vastomlijnde procedures, worden relatief weinig genomen.

6 Afhandeling van aangiften door politie en justitie

In het vorige hoofdstuk is duidelijk geworden dat de meeste bedrijven een lage pet op hebben van de strafrechtelijke afhandeling van criminaliteit waarvan zij slachtoffer worden. In het bijzonder zijn zij kritisch over de rol van de politie. Bedrijven hebben ons verteld dat de politie zelden of nooit actie onderneemt op hun aangiften. Als er al opsporing en vervolging plaatsvinden, zijn bedrijven hiervan doorgaans niet op de hoogte of ze zijn ontevreden over het resultaat (er volgt bijvoorbeeld geen veroordeling of de opgelegde straf wordt te laag bevonden).

In dit hoofdstuk proberen we meer zicht te krijgen op wat er concreet gebeurt met aangiften van interne criminaliteit bij politie en justitie. In eerste instantie kijken we naar de aangiften die bedrijven hebben gedaan bij de politie en in hoeverre deze zijn opgehelderd (paragraaf 6.2). Vervolgens gaan we na wat er met eventuele verdachten is gebeurd. Heeft er een veroordeling plaatsgevonden en zo ja, welke straf is aan hen opgelegd (paragraaf 6.3)? Alvorens hiertoe over te gaan, beschrijven we in paragraaf 6.1 eerst enige kwesties die verband houden met de dataverzameling. We besluiten dit hoofdstuk met een samenvatting en conclusie (paragraaf 6.4).

6.1 Meetkwesties

Wij hebben 139 bedrijven bevraagd over hun ervaringen met interne criminaliteit. In veel gevallen hadden deze bedrijven meer dan één vestiging. Voorzover wij over deze vestigingen hebben gesproken (respondenten hadden niet altijd zicht op alle vestigingen), hebben we deze op een lijst gezet (geordend per politieregio). In totaal gaat het om 350 vestigingen. Daarna hebben we de betreffende politieregio's benaderd met de vraag of zij wilden nagaan in hoeverre ze in de periode 1-1-2002 tot en met 31-12-2004 aangiften hebben ontvangen van de genoemde bedrijven. Hierbij hebben we geen onderscheid gemaakt naar interne of externe aangiften, maar simpelweg alle aangiften opgevraagd. We hebben de politieregio's wel gevraagd aan te geven of uit de aangifte blijkt dat sprake is van (mogelijke) interne betrokkenheid. Interne betrokkenheid blijkt niet altijd uit de aangifte. In sommige gevallen konden wij echter beschikken over informatie uit de bedrijven dat bij één of meer van hun aangiften concreet of vermoedelijk sprake was van interne betrokkenheid. Door deze informatie te leggen naast de gegevens die we via de politie verkregen, waren we in staat om achteraf nog een aantal aangiften als 'intern' te labelen.

6.1.1 Dataverzameling bij bedrijven

Tijdens de interviews bij bedrijven hebben we aan respondenten gevraagd of zij bereid waren om proces-verbaalnummers (pv-nummers) van aangiften aan ons beschikbaar te stellen, indien deze aangiften betrekking hadden op interne misdrijven. Deze pv-nummers hebben wij gebruikt om in vóórkomende gevallen de via de politie verkregen aangiften als 'intern' te kunnen labelen (zodat we deze als aparte categorie kunnen behandelen in het onderzoek). Van de 139 bedrijven die wij hebben bevraagd, hebben er 78 (56%) in de afgelopen jaren (vanaf 1-1-2002) te maken gehad met één of meer gevallen van interne criminaliteit waarvan ze ook aangifte hebben gedaan bij de politie. Van deze 78 bedrijven waren er 52 aanvankelijk bereid om de betreffende pv-nummers aan ons beschikbaar te stellen. Uiteindelijk hebben we van slechts 26 bedrijven deze informatie ook daadwerkelijk ontvangen. Omgerekend betekent dit dat we van één op de drie (relevante) bedrijven pv-nummers van interne aangiften hebben ontvangen (26 van de 78). In een aantal gevallen ging het hierbij (per bedrijf) ook om een geringer aantal interne aangiften dan aangegeven tijdens de interviews. Van deze 26 bedrijven hebben we in totaal 71 pv-nummers ontvangen. Wij vermoeden dat er verschillende oorzaken ten grondslag liggen aan deze uitval:

- In een aantal gevallen gaven respondenten tijdens het interview al aan dat ze niet bereid waren om de pv-nummers beschikbaar te stellen, omdat ze die informatie te vertrouwelijk vonden of omdat

ze niet wisten waar deze informatie zich in de organisatie bevond of omdat ze geen zin hadden hier werk van te maken;
- Van de respondenten die tijdens het interview aangaven bereid te zijn ons de betreffende pv-nummers te verstrekken, was het grootste deel niet in staat of bereid om deze informatie ten tijde van het interview (of direct na afloop) aan ons te verstrekken. Vaak kwam het er ook gewoon niet van. Deze respondenten hebben we later (tot twee keer toe) per e-mail en/of telefonisch benaderd met de vraag deze gegevens alsnog aan ons te verstrekken. Slechts in een beperkt aantal gevallen is hierop een respons gevolgd. Soms was de respons ook niet bruikbaar. Factoren die hierbij een rol hebben gespeeld zijn onder andere:

1 Soms bleek er alsnog weerstand te bestaan om deze informatie aan ons beschikbaar te stellen (bij de respondent zelf of bij anderen in het bedrijf);
2 Soms dachten respondenten dat er aangifte was gedaan, maar bleek later dat hiervan geen sprake was (of dat de aangifte was ingetrokken);
3 Soms was er wel een melding gedaan bij de politie, maar was er geen aangifte ondertekend (voor veel respondenten is het onderscheid tussen een melding en een aangifte niet helder);
4 Soms bleek dat een andere partij de aangifte had verzorgd, bijvoorbeeld de verlader of de transporteur;
5 Soms bleken de aangiften onvindbaar in het bedrijf of kostte het de respondent teveel moeite om deze te achterhalen (vooral als deze gegevens bij een andere afdeling of bij andere vestigingen lagen). Wij denken dat vooral deze laatste factor -teveel moeite- een grote rol heeft gespeeld bij de uitval;
6 Soms ontvingen we wel gegevens van bedrijven, maar was de informatie voor ons onbruikbaar, bijvoorbeeld omdat het zowel externe als interne aangiften betrof (waaruit we niet de interne aangiften konden filteren) of omdat de tijdperiode niet overeenkwam (bijvoorbeeld aangiften van vóór 1-1-2002) of omdat het geen pv-nummers betrof, maar bijvoorbeeld parketnummers.

Van de 71 pv-nummers die we via de bedrijven hebben verkregen, hebben we er slechts zeventien kunnen matchen met de politiegegevens. In zeven van deze zeventien gevallen bleek ook al uit de aangifte van de politie dat er sprake was van interne betrokkenheid. Een belangrijke verklaring voor de magere oogst ten aanzien van het matchen van pv-nummers is het feit dat we, om verschillende hierna in paragraaf 6.1.2 nog te noemen redenen, slechts een deel van alle aangiften van de politieregio's hebben ontvangen. Daarnaast speelt een rol dat bedrijven in deze sector ook aangifte doen van strafbare feiten buiten de (politie)regio('s) waar ze gevestigd zijn. Dit heeft te maken met het feit dat veel criminaliteit transportgerelateerd is. Deze incidenten worden vaak buiten de 'eigen' politieregio aangegeven. Het was voor ons ondoenlijk deze aangiften bij de politie te achterhalen.[56] Hierdoor missen we veel aangiften van met name transportgerelateerde criminaliteit.
Op basis van de informatie die respondenten bij bedrijven ons tijdens de interviews hebben verschaft, waren we in staat om nog eens 33 door de politie verzamelde aangiften als 'intern' te labelen. Hiervan waren er dertien ook al als intern gelabeld door de politie. Op basis van de door bedrijven verstrekte gegevens hebben we in totaal dus dertig aangiften (aanvullend) als intern kunnen labelen.[57]

Al met al moeten we concluderen dat het verzamelen van aangiftegegevens bij bedrijven ons een magere oogst heeft opgeleverd.

6.1.2 Dataverzameling bij de politie

[56] De dataverzameling bij bedrijven (het achterhalen van de pv-nummers) en de dataverzameling bij de politie overlapten in de tijd, waardoor we de pv-nummers van bedrijven niet konden voorleggen aan de politieregio's.
[57] (17-7) + (33-13) = 30.

Om de aangiftegegevens te verkrijgen, hebben we (bijna) alle politieregio's in Nederland en ook de KMar op Schiphol benaderd.[58] Van de in totaal 24 benaderde regio's hebben er 22 gegevens aangeleverd. De regio Flevoland hebben we niet op tijd kunnen bereiken en de regio Kennemerland hebben we wel kunnen bereiken, maar deze regio bleek niet in staat om binnen de gestelde tijd gegevens aan te leveren. Hierdoor missen we de aangiften van 25 (van de 350) bedrijfsvestigingen.
De wijze waarop we de gegevens hebben verzameld, varieert soms per politieregio. Dit heeft te maken met ons streven om de kans op een positieve en tijdige respons in alle betrokken regio's te maximaliseren. In veruit de meeste gevallen gaven politieregio's er de voorkeur aan om zelf de gegevens uit de betreffende politiesystemen te halen en voor ons te inventariseren. Deze regio's ontvingen van ons een lijst van bedrijfsnamen en vestigingsplaatsen in hun regio alsmede een Excel invulformulier waarin de gevonden gegevens verwerkt konden worden. Enkele regio's (drie) gaven er de voorkeur aan alle relevante stukken (processen-verbaal van aangifte, verdachtenverhoren en dergelijke) uit te printen en aan ons op te sturen. Die hebben we vervolgens zelf verwerkt. In één regio (Haaglanden) hebben we ook zelf de gegevensverzameling uitgevoerd, omdat één van de onderzoekers kennis had van en ook toegang had tot de relevante informatiesystemen aldaar.
We hebben aan de politieregio's gevraagd om per aangifte de volgende gegevens voor ons te noteren: het aangiftenummer, de datum van de aangifte, de strafbare feiten, eventuele buitgegevens, een indicatie van interne betrokkenheid, een indicatie van verdachten die het bedrijf bij het doen van de aangifte al op het oog had, de ophelderingsindicatie en de personalia van eventuele verdachten.[59]
Net als hiervoor bij de bedrijven is de dataverzameling bij de politieregio's niet zonder problemen verlopen. De volgende problemen deden zich voor:

- Een belangrijk deel van de aangiften van bedrijven is niet terug te vinden, omdat de regio waarin het bedrijf gevestigd is, heel vaak niet dezelfde is als de regio waar het bedrijf aangifte heeft gedaan. We noemden dit punt hiervoor al. De dataverzameling bij de politie beperkt zich derhalve tot de aangiften van bedrijven in de 'eigen' politieregio (dat wil zeggen daar waar bedrijven een vestiging hebben);
- We hebben bovendien het sterke vermoeden dat niet alle voor ons relevante aangiften die wel in de politiesystemen voorkwamen, ook daadwerkelijk aan ons zijn doorgegeven. De belangrijkste oorzaken hiervoor zijn wellicht de volgende:

1 Het identificeren van (de juiste) bedrijven leverde vaak problemen op. De namen van bedrijven zoals wij die hebben aangeleverd kwamen niet altijd overeen met de namen die bedrijven zelf, of medewerkers namens die bedrijven, hanteren. Zo hebben werkmaatschappijen van een holding vaak uiteenlopende namen. Dit probleem werd nog versterkt door het feit dat de politie in haar registraties doorgaans geen controle uitvoert op de uniciteit van rechtspersonen. Dit betekent dat bijvoorbeeld Jansen Transport in de registratie van de politie vele malen kan vóórkomen onder verschillende namen (bijvoorbeeld als Jansen, Jansen BV, Jansen Transport, Jansen Transport BV, Jansen Logistiek, et cetera). Ook ten aanzien van de vestigingsadressen deden zich soortgelijke problemen voor. Dit maakte het zoeken naar aangiften van bedrijven in de politiesystemen tot een ingewikkelde en tijdrovende activiteit;
2 Door de hiervoor genoemde problematiek, maar ook door de wijze waarop de huidige politiesystemen zijn ingericht, is het zoeken naar aangiften van geselecteerde bedrijven voor de meeste politiekorpsen een hels karwei. Om onze zoekvraag te kunnen beantwoorden moesten verschillende gegevensbestanden worden geraadpleegd, waarbij alle zoekslagen handmatig gemaakt moesten worden. Verschillende politiemedewerkers die het uitvoerende werk hebben gedaan, hebben ons gemeld dat het een enorme klus was om de gevraagde gegevens op te zoeken en te verwerken. Als we

[58] Alleen de politieregio Gooi- en Vechtstreek hebben we niet benaderd, omdat zich in deze regio geen vestigingen bevonden van bedrijven uit onze steekproef (waar we tijdens de interviews over gesproken hebben).
[59] We hebben ook nog overwogen om te vragen naar eventuele opsporingsactiviteiten en de aard ervan. Hiervan hebben we afgezien, omdat het enerzijds heel lastig is om deze activiteiten eenduidig te (laten) classificeren, maar vooral ook omdat wij verwachtten dat een dergelijke vraag tot een verhoogd 'afhaakrisico' bij de politie zou leiden; het beantwoorden van deze vragen met behulp van de huidige politiesystemen vergt een enorme inspanning.

kijken naar de output die verschillende regio's hebben aangeleverd, moeten we constateren dat sommige medewerkers zich consciëntieuzer van deze taak hebben gekweten dan andere. Er zijn regio's waarvan we bijna met zekerheid kunnen zeggen dat we slechts een marginaal deel van alle voor ons relevante aangiften aangereikt hebben gekregen.

We moeten daarom concluderen dat ook de dataverzameling bij de politie niet zonder problemen is verlopen. Niettemin hebben we in totaal 523 aangiften verzameld, waarvan we er 161 als intern hebben kunnen labelen. In aanvulling op de aangiften die de politie als intern heeft aangemerkt en de aangiften die we met behulp van de informatie uit bedrijven als intern hebben kunnen aanmerken, hebben we ook nog een aantal aangiften als intern gelabeld als sprake was van verduistering (Sr321, Sr322). Deze aangiften werden door de politie niet in alle gevallen als intern aangemerkt.

6.1.3 Dataverzameling bij justitie

Om na te gaan op welke wijze het Openbaar Ministerie (OM) en de Rechterlijke Macht (RM) hebben gereageerd op verdachten van 'interne' aangiften, hebben we deze verdachten 'opgezocht' in het Justitieel Documentatiesysteem (JDS).[60] Het gaat in totaal om 120 personen die gekoppeld zijn aan 75 interne aangiften. Als we deze verdachten aantroffen, hebben we van hen een justitieel uittreksel opgevraagd.
Het voordeel van het JDS is dat deze databank een landelijke dekking heeft. Het wordt gevoed vanuit de arrondissementen. Er is echter ook een nadeel: de informatie die per verdachte kan worden opgevraagd is beperkt. Grofweg kan de volgende informatie worden verkregen: de inschrijving van een strafzaak ter parket (en een omschrijving van de strafbare feiten), de eventuele afdoening door een Officier van Justitie (OvJ) en de aard hiervan (sepot, transactie) en de eventuele afdoening door een rechter en de aard hiervan (veroordeling, strafsoort en strafmaat). Als een zaak nog in behandeling is, kan dit worden afgeleid uit het feit dat deze is ingeschreven ter parket zonder dat een beslissing bekend is van een OvJ of een rechter. De hier genoemde informatie betreft de informatie per strafzaak. Een uittreksel van een persoon kan informatie over meer dan één strafzaak bevatten.
Een probleem van de beperkte informatie in het JDS is dat er op zaaksniveau geen koppeling gelegd kan worden naar de politiegegevens (zoals het pv-nummer van de aangifte). Dit betekent dat wij op *face value* een check hebben moeten uitvoeren om na te gaan of de aangetroffen strafzaken van verdachten respectievelijk veroordeelden betrekking hadden op de aangiften die wij van de politie hadden ontvangen. Dit was soms een lastige klus, omdat allerhande zaakgegevens (zoals strafbare feiten, pleegdata en dergelijke) in het JDS niet noodzakelijkerwijs overeenkomen met de gegevens zoals aangeleverd door de politie. Vooral als er meer verdachten waren, was het soms lastig om de koppeling te maken, omdat bijvoorbeeld verdachte één voor andere feiten is vervolgd dan verdachte twee. Of verdachte één is wel vervolgd en verdachte twee niet, et cetera. We zijn er niettemin in geslaagd in veruit de meeste gevallen de aangifte op *face value* te koppelen aan de strafzaak (op basis van alle beschikbare informatie in beide bronnen). De twijfelgevallen zijn op de vingers van één hand te tellen

6.1.4 Generaliseerbaarheid van bevindingen

Het aanvankelijke idee om na afloop van de bevraging bij de bedrijven ook nog 'even' de aangiften van deze bedrijven bij de politie na te lopen (en daarna bij justitie), is achteraf bezien royaal naïef gebleken. De vele problemen die hierbij zijn opgetreden, hadden we niet voorzien. Een aantal van deze problemen laat zich uiteindelijk wel oplossen, maar het kader van dit onderzoek is hiervoor te beperkt. Ons overzicht van aangiften (en de eventuele politiële en justitiële activiteiten die hierop gevolgd zijn) is zeer waarschijnlijk verre van compleet. Dit leiden we onder meer af uit het feit dat we veel aangiften van bedrijven niet hebben teruggevonden in de gegevens van de politie. Het

[60] Ons selectiecriterium is: verdachten die gekoppeld zijn aan 'interne' aangiften. Als er van een strafbaar feit meer verdachten zijn, is het voor ons meestal niet na te gaan welke verdachten intern zijn en welke (eventueel) extern. Dit onderscheid hebben we dan ook niet gemaakt.

omgekeerde komt echter ook regelmatig voor: aangiften die we van de politie hebben ontvangen en waar bedrijven ons niet over verteld hadden.
Een en ander roept de vraag op naar de generaliseerbaarheid van de bevindingen die we hierna beschrijven. Wij zijn van mening dat de 'uitval' van aangiften geen systematisch karakter heeft, op één uitzondering na; de aangiften die bedrijven buiten de eigen (vestigings)regio hebben gedaan zijn systematisch ondervertegenwoordigd in onze verzameling. We kunnen echter geen redenen bedenken waarom deze aangiften anders afgehandeld zullen worden dan aangiften die bedrijven doen in de 'eigen' politieregio. Daarom menen we dat de bevindingen die we hierna bespreken weliswaar beperkt zijn voor wat betreft het soort aangiften dat we verzameld hebben (transportgerelateerde criminaliteit is zeer waarschijnlijk ondervertegenwoordigd), maar wel een goede indicatie geven van de wijze waarop politie en justitie de aangiften afhandelen.

6.2 Aangiften en opsporing

In tabel 11 hebben we de aangiften beschreven die we via de politieregio's hebben verkregen. In totaal hebben we 523 aangiften verzameld van bedrijven uit onze steekproef. Deze aangiften hebben betrekking op de periode 2002-2004. In totaal 161 aangiften hebben we als intern kunnen labelen op basis van enige bron (ruim 30%). Dit is zeer waarschijnlijk een onderschatting, omdat onze kennis van de meeste aangiften te gering is om vast te kunnen stellen of sprake is van interne betrokkenheid. Aangiften waarbij geen interne betrokkenheid is vastgesteld, duiden we hier aan als 'overige aangiften'. Wanneer we kijken naar de omschrijvingen en achtergronden van de 'overige' aangiften, kunnen we ons niet aan de indruk onttrekken dat een significant deel hiervan waarschijnlijk ook een interne component heeft. Hierbij gaat het om criminele feiten waarvan het moeilijk is voor te stellen dat er géén interne personen betrokken zijn of om feiten waarbij dit op zijn minst heel waarschijnlijk is. De categorie 'overige aangiften' zal derhalve enigszins vervuild zijn met aangiften die ook betrekking hebben op interne incidenten.

Tabel 11 Beschrijving van (interne) aangiften en ophelderingsindicatie

	Interne aangiften	*Overige aangiften**
Aantal absoluut (n)	161	362
Delictcategorie (%)		
Verduistering	60%	0%
(Overige) eenvoudige diefstal	15%	37%
Inbraak in pand	12%	26%
Inbraak in voertuig	4%	25%
Diefstal van vrachtauto (vaak inclusief lading)	3%	5%
Vernieling	1%	2%
Overige	1%	1%
Fraude	2%	1%
Overige inbraak	2%	3%
Soort buit (%)		
Handelsgoederen	70%	48%
Geld	11%	3%
Bedrijfsmiddelen	7%	22%
Vrachtauto´s (vaak inclusief lading)	4%	4%
Privé-spullen van werknemers	3%	2%
Geen buit/niet van toepassing/onbekend	7%	22%

Waarde-indicatie van de buit (%)		
Minder dan € 250	13%	12%
€ 250 - € 10.000	54%	46%
Meer dan € 10.000	22%	12%
Waarde onbekend	4%	8%
Buit niet van toepassing	7%	22%
Bedrijf heeft verdachte(n) op het oog (%)	50%	3%
Opgehelderde aangiften (%)	49%	3%

* overige aangiften: dit zijn deels 'externe' aangiften en deels aangiften waarvan we de interne status niet hebben kunnen vaststellen.

De delicten waarop de interne aangiften betrekking hebben wijken af van de delicten waarop de overige aangiften betrekking hebben: 60% van de interne aangiften houdt verband met verduistering. Deze categorie komt bij de overige aangiften uiteraard niet voor. Immers, verduistering duidt per definitie op interne betrokkenheid. Daarnaast bestaat 15% van de interne aangiften uit overige diefstalgevallen. Daarmee komt het percentage eenvoudige diefstallen bij de interne aangiften op 75%. Bij de overige aangiften ligt dit percentage op 37%. Van de interne aangiften heeft 21% betrekking op inbraak van enige soort (als we diefstal van vrachtauto's hier ook meetellen). In meer dan de helft van deze gevallen gaat het om inbraak in een pand (loods, kantoor, garage en dergelijke). Bij de overige aangiften ligt het percentage inbraken met 59% bijna drie keer zo hoog als bij de interne aangiften. Hierbij gaat het vooral om inbraken in panden en inbraken in voertuigen (meestal vrachtauto's, vaak ladingdiefstal, maar ook veel diefstallen van privé-spullen van de chauffeur). Aangiften van andere vormen van criminaliteit komen maar heel weinig voor. Zowel bij de interne als bij de overige zaken gaat het om 4% van de aangiften.
Dit beeld bevestigt onze bevindingen bij de bedrijven: als het gaat om interne criminaliteit, is men vooral gefocust op (interne) diefstal. Het grootste deel van de interne aangiften heeft hierop betrekking. Als grootste (niet-interne) criminaliteitsprobleem zien bedrijven de ladingdiefstallen (door middel van inbraken in loodsen en vrachtauto's). Deze categorieën vormen ook de meerderheid van de overige aangiften. Dat het percentage aangiften van inbraken in panden ongeveer gelijk is aan het percentage inbraken uit voertuigen, bevestigt ons vermoeden dat de laatste categorie ondervertegenwoordigd is. Immers uit de bevraging van bedrijven kwam naar voren dat transportgerelateerde inbraken vaker voorkomen dan pandgerelateerde inbraken. Dat van andere zaken dan diefstal en inbraak nauwelijks aangifte wordt gedaan, is ook een bevestiging van wat bedrijven ons eerder verteld hebben, namelijk dat men in deze gevallen meestal een interne afhandeling verkiest en dus geen aangifte doet bij de politie.
We hebben de aangiften ook gerangschikt naar het type buit (indien relevant) en de waarde van de buit (in euro's). Ten aanzien van dit laatste hebben we drie grove categorieën gehanteerd: kleine buit (minder dan 250 euro), middelmatige buit (250 tot 10.000 euro) en grote buit (meer dan 10.000 euro). De grenzen zijn willekeurig en de toekenning is vaak op basis van een schatting onzerzijds, gebaseerd op de door de politie aangeleverde gegevens. De 'waarde van de buit' moet dan ook worden gezien als een indicatieve grootheid.
We zien in tabel 11 dat de buit bij interne aangiften in veruit de meeste gevallen (70%) bestaat uit handelsgoederen. Ook geld is regelmatig het doelwit (11%). Deze laatste gevallen hebben vooral betrekking op bedrijven die met remboursementen werken (zoals koeriersbedrijven). De andere typen buit komen veel minder vaak voor. De hiervoor aangehaalde diefstallen en verduisteringen hebben dus vooral betrekking op handelsgoederen. Bij de overige aangiften zien we dat bedrijfsmiddelen vaker de buit vormen. Hierbij gaat het veelal om zaken als computerapparatuur, navigatiesystemen en dergelijke die gestolen worden bij inbraken in kantoren en auto's. Bij de overige aangiften komt het ook vaker voor dat er geen buit is (dit zijn niet-geslaagde pogingen tot inbraak). Als we kijken naar de waarde van de buit, kunnen we vaststellen dat bij circa de helft van de interne aangiften (54%) sprake

is van een ‘gemiddelde’ buit. Bij een klein deel van de aangiften is sprake van een geringe buit (minder dan 250 euro). In iets meer dan één op de vijf gevallen (22%) is sprake van een grote buit (meer dan 10.000 euro). Bij de overige aangiften ligt de gemiddelde omvang van de buit iets lager. Dit heeft te maken met het feit dat het aandeel onvoltooide delicten (pogingen) hier groter is. Al met al hebben we geen redenen om aan te nemen dat de interne aangiften afwijken van de overige aangiften als het gaat om de aard en omvang van de buit.
Het grootste verschil tussen de interne en de overige aangiften is dat bij de eerste groep veel vaker sprake is van bedrijven die al verdachten op het oog hebben (50 tegen 3%). Dit verschil ligt voor de hand, omdat op basis van deze informatie politiefunctionarissen in staat waren om een aangifte als intern aan te merken. We zien vervolgens dat het percentage opgehelderde interne aangiften ongeveer op hetzelfde niveau ligt (opgehelderd betekent doorgaans dat er verdachten zijn gehoord in het kader van een aangifte).[61] Deze bevinding betekent niet dat alle aangiften waarbij bedrijven vooraf verdachten op het oog hadden, ook zijn opgehelderd. In totaal hebben we 80 interne aangiften gevonden waarbij door het bedrijf één of meer verdachten zijn genoemd. Van deze 80 zijn er 65 door de politie opgehelderd. Het niet-ophelderen had soms te maken met bewijstechnische redenen (gebrek aan bewijs). Soms ook vond er geen nadere opsporingsactiviteit plaats. Zo meldde een politieregio een geval waarin een verdachte niet kwam opdagen voor een verhoor, waarna men het er maar bij liet zitten. Ook kwam het enkele malen voor dat het bedrijf ervoor koos de zaak verder intern en/of civielrechtelijk af te handelen. Naast de hiervoor genoemde 65 zaken, heeft de politie ook nog eens 13 interne aangiften opgehelderd, waarbij het bedrijf niet vooraf al verdachten op het oog had (of beter gezegd: waarbij dit niet bleek uit de aangifte). Met andere woorden, de verzameling opgehelderde interne aangiften bestaat voor het overgrote deel uit zaken waarbij het bedrijf zelf de verdachte(n) heeft aangeleverd (65 van de 78 gevallen) en voor een klein deel (13 van de 78 gevallen) uit zaken waarbij bedrijven niet vooraf al verdachten op het oog hadden (althans: waar dit niet bleek uit de aangifte).
Als we, ten slotte, kijken naar de categorie overige aangiften, zien we dat slechts een zeer gering deel van deze aangiften is opgehelderd (3%). Het gaat om tien opgehelderde aangiften. In vier gevallen ging het om aangiften waarbij bedrijven vooraf verdachten op het oog hadden, in zes gevallen was dit niet aan de orde.
Ten aanzien van de afhandeling van interne aangiften door de politie is onze conclusie dat opheldering vooral afhankelijk is van de vraag of bedrijven zelf verdachten kunnen aandragen. Als ze dit niet kunnen, is de kans dat een aangifte wordt opgehelderd heel erg klein. Echter, ook wanneer bedrijven verdachten aandragen, leidt dit niet altijd tot opheldering.

6.3 Vervolging en berechting van verdachten

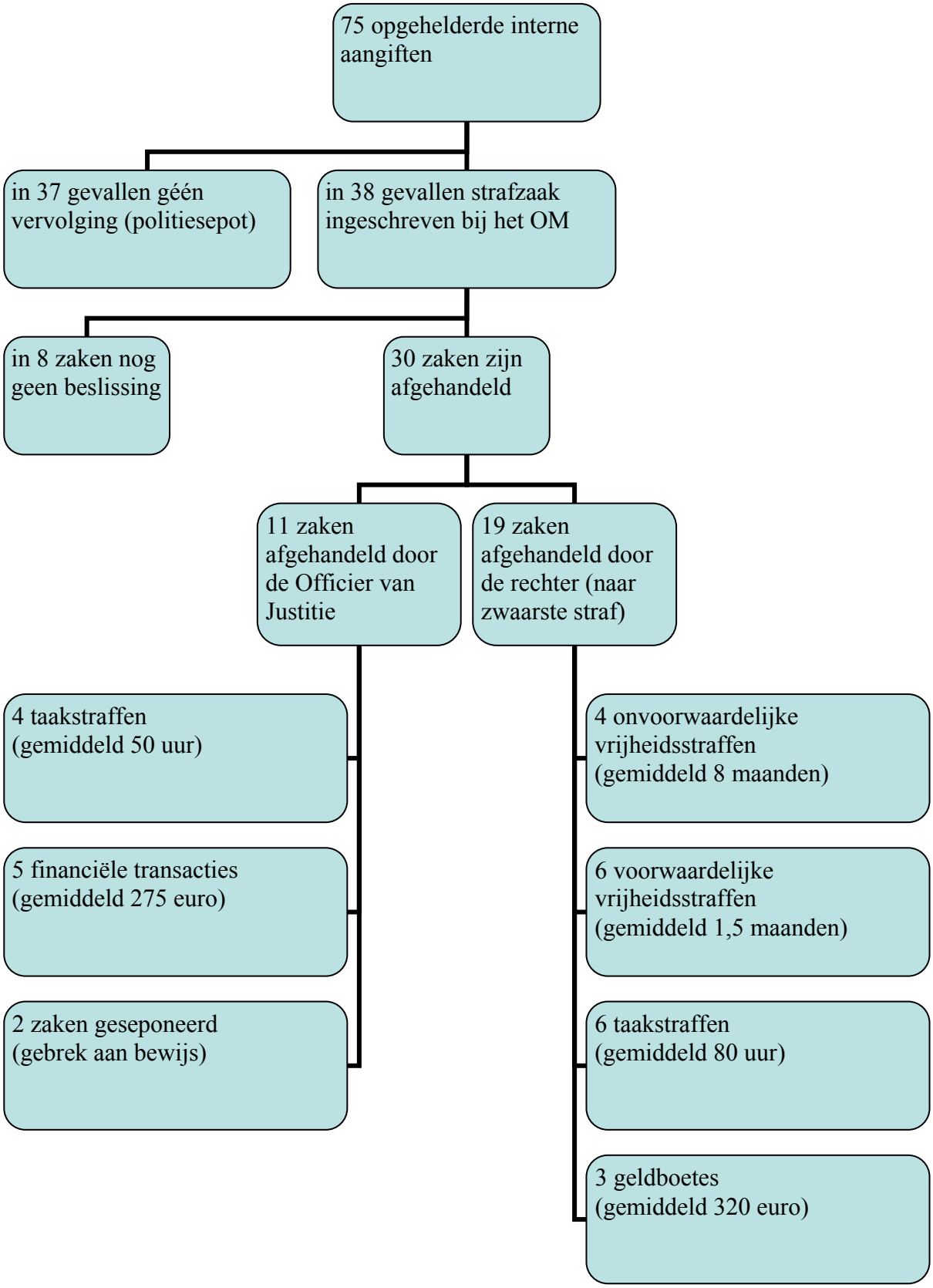
Van de 161 interne aangiften die wij bij de politie hebben aangetroffen zijn er 78 opgehelderd. Hiervan beschikken we in 75 gevallen ook over de verdachtengegevens. De opgehelderde zaken wijken qua delictsoort, aard en waarde van de buit niet of nauwelijks af van de niet-opgehelderde aangiften. Het is dus niet zo dat bijvoorbeeld zaken met een omvangrijke buit eerder of vaker worden opgehelderd dan ‘kleinere’ feiten. In 57 van de 75 gevallen is er één verdachte bekend, in de overige 18 gevallen zijn er twee of meer verdachten bekend. We hebben ervoor gekozen de justitiële afhandeling van opgehelderde aangiften op zaaksniveau te beschrijven en niet op het niveau van individuele verdachten of veroordeelden. Dit geeft ons inziens een beter beeld van de wijze waarop justitie met deze zaken omgaat.[62] Aangezien de afhandeling per verdachte of veroordeelde in een zaak

[61] De conceptualisering en operationalisering van de term ‘opheldering’ is niet zonder problemen. Aangezien deze problemen niet of nauwelijks van invloed zijn op de door ons gepresenteerde bevindingen, laten we beschouwingen hieromtrent achterwege.
[62] Vooral in zaken met meer verdachten komt het vaak voor dat sommige verdachten wel worden vervolgd en andere niet. Bovendien worden verdachten vaak niet voor dezelfde feiten vervolgd (bijvoorbeeld verdachte 1 voor heling en verdachte 2 voor diefstal). Voorts bepaalt ook de rol in de samenwerking tussen de verdachten de strafeis die de OvJ aan specifieke verdachten zal opleggen en de veroordeling die hierop mogelijk volgt. Om deze redenen ligt het minder voor de hand om de afdoening van zaken op persoonsniveau te beschrijven.

kan verschillen, gaan we telkens uit van de 'zwaarste' beslissing. Dus als er drie verdachten zijn waarvan er maar één is vervolgd, dan spreken we over een zaak waarin een vervolging heeft plaatsgevonden. Als er twee verdachten zijn, waarvan er één een taakstraf (meestal een werkstraf) heeft gekregen en de ander een vrijheidsstraf, dan spreken we over een zaak waarin een vrijheidsstraf is opgelegd.
In het stroomschema van figuur 4 wordt weergegeven hoe de zaken werden afgehandeld. Van de 75 opgehelderde interne zaken hebben we in 37 gevallen (49%) óf de persoon óf de zaak niet kunnen terugvinden in het JDS. In het eerste geval gaat het om personen van wie geen strafzaken vóórkomen in het JDS.[63] In het tweede geval gaat het om personen die weliswaar vóórkomen met strafzaken in het JDS, maar die niet werden vervolgd voor de zaak waar het ons om ging. In bijna de helft van de 75 gevallen werd de strafzaak dus niet ingeschreven bij het parket van het OM. De meest voorkomende sepotreden was (voor zover bij ons bekend) dat de zaak door het bedrijf intern en/of civielrechtelijk werd afgehandeld. Daarnaast zijn er ook enkele gevallen waarin het bewijs onvoldoende bleek. Van een aantal opgehelderde aangiften weten we niet waarom er geen vervolging van verdachten heeft plaatsgevonden.

Figuur 4 Afhandeling van opgehelderde interne aangiften (stroomschema)

[63] Een verklaring voor het feit dat we bepaalde personen niet hebben kunnen aantreffen in het JDS, is mogelijk gelegen in het verkeerd gespeld zijn van namen, onjuiste geboortedata en dergelijke. We hebben hierop een controle uitgevoerd. De kans dat personen op deze gronden niet gematcht konden worden in het JDS is volgens ons te verwaarlozen.


75 opgehelderde interne aangiften
in 37 gevallen géén vervolging (politiesepot)
in 38 gevallen strafzaak ingeschreven bij het OM
in 8 zaken nog geen beslissing
30 zaken zijn afgehandeld
11 zaken afgehandeld door de Officier van Justitie
19 zaken afgehandeld door de rechter (naar zwaarste straf)
4 taakstraffen (gemiddeld 50 uur)
5 financiële transacties (gemiddeld 275 euro)
2 zaken geseponeerd (gebrek aan bewijs)
4 onvoorwaardelijke vrijheidsstraffen (gemiddeld 8 maanden)
6 voorwaardelijke vrijheidsstraffen (gemiddeld 1,5 maanden)
6 taakstraffen (gemiddeld 80 uur)
3 geldboetes (gemiddeld 320 euro)

Van de 38 overblijvende zaken waren er op het moment van dataverzameling nog acht in behandeling. Van de overige dertig zaken zijn er elf afgedaan door de OvJ en negentien door de rechter. De OvJ heeft in twee gevallen alsnog geseponeerd (om bewijstechnische redenen) en in de overige negen gevallen is vier keer een taakstraf opgelegd (werkstraffen variërend van 20 tot 60 uur) en vijf keer een financiële transactie getroffen (bedragen variërend van 190 tot 360 euro).
De zaken die zijn afgedaan door de rechter hebben in alle gevallen geleid tot veroordelingen. Bij de beschrijving in figuur 4 zijn we uitgegaan van de 'zwaarste' sanctie die is opgelegd in een bepaalde zaak. We onderscheiden van zwaar naar licht: onvoorwaardelijke vrijheidsstraf, voorwaardelijke vrijheidsstraf, taakstraf en geldboete. We zien in figuur 4 dat in vier zaken onvoorwaardelijke vrijheidsstraffen zijn opgelegd (variërend van anderhalve maand tot anderhalf jaar). In vier zaken zijn aan verdachten voorwaardelijke vrijheidsstraffen opgelegd (variërend van één week tot een half jaar), vaak in combinatie met een taakstraf (werkstraffen van 60 tot 220 uur). In zes gevallen bestond de zwaarste sanctie uit een taakstraf (variërend van 30 tot 180 uur). In drie gevallen werd een geldboete opgelegd (van 225 tot 400 euro). In figuur 4 is niet vermeld dat in vier van de negentien gevallen als bijkomende maatregel de verplichting tot schadevergoeding werd opgelegd (de bedragen variëren van 200 tot 2.000 euro).
We hebben vergelijkbare afdoeningen samengevoegd om een samenvattend beeld te kunnen presenteren van de wijze waarop strafzaken zijn afgedaan. In tabel 12 zijn de sepotzaken (door de politie en het OM) samengevoegd en daarnaast zijn de (door het OM en de RM) opgelegde taakstraffen, geldboetes en vrijheidsstraffen opgenomen. De acht zaken die nog in behandeling waren, hebben we hier buiten beschouwing gelaten. We zien in tabel 12 dat de meerderheid van de zaken werd geseponeerd (58%). De overige afdoeningen zijn min of meer gelijkelijk verdeeld over de drie sanctiemodaliteiten: geldboete, taakstraf en vrijheidsstraf (elk 12 tot 15%).

Tabel 12 Samenvatting van justitiële afdoeningen*

	Aantal zaken	Percentage
Géén vervolging (sepot politie/OM)	39	58%
Geldboete (OM/Rechter)	8	12%
Taakstraf (OM/Rechter)	10	15%
Voorwaardelijke vrijheidsstraf	6	9%
Onvoorwaardelijke vrijheidsstraf	4	6%
Totaal	67	100%

* alleen de 'zwaarste' beslissing/sanctie in een zaak is telkens gepresenteerd. Lopende zaken zijn buiten beschouwing gelaten.

We hebben ook nog onderzocht of en zo ja, op welke wijze de hier genoemde afdoeningen gerelateerd zijn aan kenmerken van de strafzaak. In de meeste gevallen hebben we geen verband kunnen aantreffen.[64] De volgende waarnemingen vormen hierop een uitzondering: als de waarde van de buit laag is, wordt er alleen een taakstraf of een geldboete opgelegd. Vrijheidsstraffen komen bij deze categorie niet voor. Als er sprake is van meer dan één verdachte of van verdachten die al een strafblad hebben, is de kans iets groter dat er een vrijheidsstraf wordt opgelegd.
Tot slot nog een toelichting op de individuele verdachten respectievelijk veroordeelden. Van de 120 verdachten die de politie had gekoppeld aan de 75 opgehelderde interne aangiften, hebben we er 103 teruggevonden in het JDS. Van honderd van deze personen weten we of ze recidivist zijn (hier gedefinieerd als: het vóórkomen van strafzaken in het JDS voorafgaand aan de zaak waarvan ze in het kader van dit onderzoek verdacht werden). Van deze verdachten bleek 76% eerder voor te komen in het JDS in verband met strafzaken. De overgrote meerderheid van deze groep heeft dus géén onbeschreven strafblad. Gemiddeld hadden deze personen meer dan vijf vermeldingen van strafzaken in het JDS voorafgaand aan het feit waarin wij geïnteresseerd waren (dit laatste resultaat wordt vertekend door enkele veelplegers; mediaan is 2, modus is 1).

[64] Dit heeft waarschijnlijk mede te maken met de kleine aantallen waarop de analyses gebaseerd zijn en de beperkte zaaksgegevens die we tot onze beschikking hebben.

Ten aanzien van de vervolging en berechting van verdachten van interne criminaliteit is een belangrijke bevinding dat in de meerderheid van de door ons onderzochte zaken werd afgezien van vervolging. We hebben hierbij geen relatie gesignaleerd met de aard en de ernst van de gepleegde feiten. Als wel tot vervolging werd overgegaan, bestonden de zwaarst opgelegde sancties in de meeste gevallen uit geldboetes of taakstraffen.

6.4 Samenvatting en conclusie

Voorbehoud bij conclusies door problemen met dataverzameling
Door allerhande problemen die optraden bij de dataverzameling in deze fase, moeten we enige voorzichtigheid betrachten bij het trekken van conclusies ten aanzien van de afhandeling van aangiften door politie en justitie. We hebben bij de politie in totaal 523 aangiften van bedrijven uit onze steekproef kunnen verzamelen, waarvan we er 161 hebben kunnen labelen als intern. Hiervan werden 121 aangiften door de politie als intern gekwalificeerd op grond van informatie in de aangifte (meestal betekende dit dat het bedrijf een interne verdachte op het oog had). Daarnaast zijn dertig aangiften door ons als intern gelabeld op grond van informatie van bedrijven (pv-nummers of informatie uit interviews). Ten slotte hebben we nog tien aangiften als intern gelabeld op grond van de gebruikte wetsartikelen (verduistering: artikelen Sr321 en Sr322). We vermoeden dat een deel van de overige aangiften ook een intern karakter heeft, maar we kunnen dit niet aantonen. Door de wijze van dataverzameling zijn aangiften die bedrijven buiten de eigen (politie)regio hebben gedaan, sterk ondervertegenwoordigd. Dit betekent dat met name transportgerelateerde criminaliteit is ondervertegenwoordigd in de aangiften die wij verzameld hebben. Verder hebben we het sterke vermoeden dat sommige politieregio's consciëntieuzer zijn omgegaan met onze informatievraag dan andere. (Het verzamelen van de door ons gewenste informatie bleek voor de politie een uitermate tijdrovende klus.) Dit betekent dat de verzamelde aangiften waarschijnlijk slechts een deel vormen van alle aangiften die bedrijven uit ons onderzoek in de afgelopen jaren hebben gedaan bij de politie. We hebben geen redenen om aan te nemen dat de wijze van afhandeling van de door ons verzamelde aangiften zal afwijken van de afhandeling van aangiften die niet in onze verzameling zitten.

Afhandeling van aangiften door de politie
Als we kijken naar het soort gebeurtenissen waarop de aangiften betrekking hebben, wordt het beeld bevestigd dat uit de bedrijveninterviews naar voren kwam: aangiften van interne criminaliteit hebben vooral betrekking op verduistering (en overige diefstal) van handelsgoederen. Bij aangiften van 'externe criminaliteit' gaat het veel vaker om inbraken in gebouwen en voertuigen, waarbij ook weer vooral handelsgoederen worden gestolen, maar in veel gevallen ook bedrijfsmiddelen. De meeste aangiften hebben betrekking op delicten met een buit tussen 250 en 10.000 euro. Bij de interne aangiften gaat het in 22% van de gevallen om delicten met een grote buit (meer dan 10.000 euro).
Om een aantal redenen is het voor ons niet mogelijk om betrouwbare uitspraken te doen over het ophelderingspercentage van aangiften van interne criminaliteit. De belangrijkste reden is dat zowel onze verzameling van aangiften *totaal* als onze verzameling van *interne* aangiften niet volledig is. Met name de laatste verzameling is niet representatief, omdat politiefunctionarissen in veel gevallen aangiften als intern hebben gelabeld indien door het bedrijf interne verdachten werden genoemd. Het algehele ophelderingspercentage van alle door ons verzamelde aangiften ligt op 17%. Dit percentage ligt in de buurt van het gemiddelde ophelderingspercentage dat wordt gerealiseerd door de politie (afhankelijk van de gehanteerde verzameling delicten lag dit percentage in 2003 tussen vijftien en twintig) (Eggen et al., 2005).
Interessanter is de bevinding dat opheldering van misdrijven door de politie sterk gekoppeld is aan het gegeven dat bedrijven zelf al verdachten op het oog hebben. In 78% van de gevallen waarin een aangifte werd opgehelderd, was sprake van een bedrijf dat al een verdachte op het oog had. Bij de interne aangiften lag dit percentage zelfs op 83%. De kans dat een aangifte wordt opgehelderd als het

bedrijf zelf geen verdachten op het oog heeft, ligt in onze verzameling aangiften op 4%.[65] Echter, ook als het bedrijf al verdachten op het oog had, betekende dit niet automatisch dat het misdrijf werd opgehelderd. In 23% van deze gevallen werd het misdrijf niet opgehelderd. Factoren die hierbij een rol speelden zijn onder andere: gebrek aan bewijs, gebrek aan politieactiviteit en de wens van het bedrijf om de zaak verder intern af te handelen. De opgehelderde aangiften wijken op kenmerken niet of nauwelijks af van de niet-opgehelderde aangiften. Ook hierin vinden we een aanwijzing dat niet zozeer de aard en de ernst van een delict doorslaggevend zijn voor de opsporingsbeslissing, maar de informatie die beschikbaar is vanuit de bedrijven.

Vervolging en berechting
In meer dan de helft van de gevallen (52%) werden de opgehelderde interne aangiften (75 in onze verzameling) geseponeerd. In de meeste gevallen ging het hierbij om een politiesepot. In deze zaken werd dus niet tot vervolging overgegaan. De meest voorkomende sepotreden die wij hebben aangetroffen is dat de zaak door het bedrijf intern en/of civielrechtelijk werd afgehandeld. In enkele gevallen bleek het bewijs niet rond te krijgen.
In de gevallen waarin wel tot vervolging werd overgegaan, werd de zaak in elf gevallen door de OvJ afgehandeld (meestal door middel van een financiële transactie of een taakstraf) en in negentien gevallen door een rechter die in alle gevallen tot veroordelingen kwam. De maximale straffen varieerden van 190 euro boete tot anderhalf jaar onvoorwaardelijke gevangenisstraf.
Opvallend is dat 76% van de verdachten van de opgehelderde interne zaken al een strafblad had. Een deel van deze verdachten had zelfs een zeer uitgebreid strafblad. Hieruit mag niet de conclusie worden getrokken dat interne criminaliteit vooral wordt gepleegd door 'doorgewinterde' criminelen. Als werknemers met een strafblad zich schuldig maken aan interne criminaliteit, verhoogt dit gegeven waarschijnlijk de kans dat zij worden opgespoord en vervolgd.

Samenvattende conclusie
In het vorige hoofdstuk maakten we melding van het feit dat veel bedrijven kritiek leveren op de strafrechtelijke afhandeling van criminaliteit en in het bijzonder op de rol van de politie hierin. De vraag is nu of deze kritiek, gelet op de bevindingen van dit hoofdstuk, terecht is? Wij denken dat deze vraag met 'ja' beantwoord moet worden, zij het met enkele kanttekeningen. Impliciet of expliciet leeft bij veel bedrijven het idee dat zij, als slachtoffer van criminaliteit, door politie en justitie 'slechter' worden behandeld dan individuele burgers. Dit kwam regelmatig naar voren tijdens de interviews. Op basis van voorgaande analyse is het voor ons echter niet mogelijk hierover iets zinvols te zeggen, omdat we geen gegevens beschikbaar hebben die een systematische vergelijking mogelijk maken tussen de afhandeling van aangiften door bedrijven en door burgers. Wat we wel zien is dat het ophelderingspercentage van de interne aangiften van bedrijven in ons onderzoek nauwelijks verschilt van het ophelderingspercentage van alle aangiften die bij de politie worden gedaan (Eggen et al., 2005). In dit opzicht is er dus geen verschil tussen de behandeling van burgers en bedrijven. Overigens is deze vergelijking een moeizame, omdat de respectieve verzamelingen op belangrijke punten kunnen afwijken (bijvoorbeeld het deel van de aangiften dat betrekking heeft op zaken waarbij vooraf al een verdachte bekend is).[66] Wij hebben geen redenen om aan te nemen dat bedrijven door politie en justitie bewust slechter of anders worden behandeld dan individuele burgers. Omgekeerd hebben we echter ook geen aanwijzingen gevonden waaruit blijkt dat met name de zwaardere vormen van criminaliteit waardoor de logistieke sector regelmatig wordt getroffen, enige prioriteit genieten bij politie en justitie.
Als we kijken naar de strafrechtelijke afhandeling van interne aangiften die bedrijven hebben gedaan, constateren we:

[65] Dit lijkt ons nog een positieve schatting, omdat in deze gevallen weliswaar niet uit de aangifte bleek dat bedrijven al concrete verdachten op het oog hadden, maar wel dat bedrijven vaak beschikten over aanwijzingen. Alleen de namen van de verdachten ontbreken in deze aangiften.
[66] Vergelijk in dit verband bijvoorbeeld de ophelderingspercentages van geweldsdelicten en vermogensdelicten: 53 versus 11% (Eggen et al., 2005). Dit grote verschil wordt veroorzaakt door het feit dat bij geweldsdelicten naar verhouding veel vaker sprake is van een op voorhand bekende verdachte.

- Dat de opheldering van zaken door de politie vooral afhankelijk is van de informatie die bedrijven aanreiken over mogelijke verdachten: zonder deze informatie worden aangiften zelden opgehelderd;
- Dat in de meerderheid van de opgehelderde zaken geen vervolging van verdachten plaatsvindt;
- Dat in tweedederde van de zaken waarin vervolging heeft plaatsgevonden, de zwaarst opgelegde sanctie bestaat uit een geldboete of taakstraf (ook in gevallen waarin sprake was van een omvangrijke buit).

De hier genoemde uitkomsten kwalificeren als goed of slecht is om drie redenen lastig. In de eerste plaats ontbreekt ons de detailkennis om voor elke zaak na te kunnen gaan hoe verschillende beslissingen beoordeeld moeten worden (zoals bijvoorbeeld de opgelegde straffen in individuele strafzaken). In de tweede plaats ontbreekt een vergelijkingsgrond om de uitkomsten tegen af te zetten. In de derde plaats ontbreekt een normatief kader aan de hand waarvan we kunnen vaststellen of de prestaties boven of onder de norm zijn. Wij vermoeden dat veel van onze respondenten (van bedrijven) in de hier gepresenteerde bevindingen een onderbouwing zien van hun kritiek. Wij kunnen dit wel begrijpen, waarbij we de casuïstiek laten meewegen die we tijdens de interviews in bedrijven zo vaak zijn tegengekomen en waarover we in hoofdstuk 5 hebben gerapporteerd. De 'schrijnende' ervaringen van bedrijven met vooral de politie zijn net iets te talrijk om incidenteel genoemd te kunnen worden. Het lijkt er al met al toch op dat politie en justitie net iets minder aandacht hebben voor bedrijven als slachtoffer van criminaliteit (in vergelijking met individuele burgers die slachtoffer worden). De indicaties hiervoor zijn echter moeilijk te kwantificeren. Kortom, de prestaties van politie en justitie als onvoldoende kwalificeren is een lastige opgaaf, maar omgekeerd is het net zo moeilijk om onder de indruk te raken van de hier gepresenteerde uitkomsten.
Toch is het verhaal minder eenzijdig dan (sommige) bedrijven ons willen doen geloven, omdat zij zelf ook een rol spelen in de hiervoor gepresenteerde bevindingen. Bedrijven kiezen er in veel gevallen voor om geen aangifte te doen, omdat hen dit om allerlei redenen beter uitkomt. Daarnaast hebben we gezien dat bedrijven er vaak voor kiezen om na een aangifte alsnog een interne of civielrechtelijke weg te bewandelen. Een en ander betekent onder andere dat de informatiepositie van politie en justitie veel minder optimaal is dan mogelijk wanneer bedrijven vaker het strafrechtelijke traject zouden bewandelen. Hierdoor wordt de opsporing en vervolging van soortgelijke zaken belemmerd. Bovendien kan een werknemer die bij bedrijf A wegens een misdrijf is ontslagen nu vaak zonder veel problemen weer aan de slag bij bedrijf B, omdat dit feit nergens bekend is. De sector heeft dus wel degelijk een collectief belang bij strafrechtelijke afhandeling, vooral met het oog op de recidiverende daders die een sterk verhoogd risico vormen voor de sector. Bedrijven zijn echter ook nalatig bij het screenen van nieuw personeel. Uit het feit dat een groot deel van de door ons onderzochte verdachten een strafblad had, kunnen we afleiden dat dit gegeven blijkbaar geen belemmering voor hen is geweest om bij het betreffende bedrijf binnen te komen. Ten slotte getuigt de wijze waarop veel bedrijven gereageerd hebben (of juist niet gereageerd hebben) op onze oproep om pv-nummers te leveren voor dit deel van het onderzoek, niet van een 'sterke interesse' in de strafrechtelijke afhandeling van hun aangiften. Kortom, ook bedrijven dragen hun steentje bij aan de in hun (en ook onze) ogen magere uitkomsten van het strafrechtelijk traject.

7 Conclusies

Belangrijkste criminaliteitsprobleem in logistieke sector is gerelateerd aan grootschalige ladingdiefstal

Meer dan interne criminaliteit beschouwen bedrijven in deze sector externe criminaliteit als een probleem: tweederde van de bedrijven noemt dit een probleem waarmee ze soms tot zeer regelmatig te maken hebben. Het is vooral transportgerelateerde criminaliteit waar ze de meeste last van ondervinden. Hierbij gaat het met name om trailer- en ladingdiefstallen, maar ook om overvallen op vrachtauto's. De schade die bedrijven hiervan ondervinden ligt zowel in de hoge frequentie waarmee ze slachtoffer worden van deze misdrijven als in de hoge waarde van de goederen die doorgaans gestolen worden; het komt dus niet alleen vaak voor, de schades per geval zijn ook hoog. Overigens moet hierbij opgemerkt worden dat ook logistiek dienstverleners die het transport hebben uitbesteed hiervan last kunnen ondervinden, bijvoorbeeld omdat zij als contractpartij aansprakelijkheid dragen of omdat ze imagoschade ondervinden. We herinneren eraan dat bijna tweederde van de bedrijven in ons onderzoek geen transportfunctie heeft of deze (grotendeels) heeft uitbesteed! Als we alle transportgerelateerde incidenten uit de cijfers weg zouden laten, zou de sector er qua criminaliteit een stuk rustiger uitzien. Er vinden weliswaar met enige regelmaat ook inbraken plaats in loodsen of in kantoren van bedrijven en ook diefstallen door medewerkers in de loods komen zeer regelmatig voor, maar de schade die bedrijven hiervan ondervinden, en ook van andere vormen van (interne) criminaliteit, valt in zijn totaliteit toch veel geringer uit. Niet voor niets noemen veel bedrijven het transport als hun grootste risicofactor.

Bij grootschalige diefstal van handelsgoederen is veel vaker dan bedrijven denken (of aan ons rapporteren) sprake van interne betrokkenheid

Bedrijven beschouwen transportgerelateerde criminaliteit in hoofdzaak als een extern probleem. Het aantal gevallen waarin ze weten of vermoeden dat er sprake is van interne betrokkenheid, is gering. Diefstal van handelsgoederen, en dan met name grootschalige ladingdiefstal (waar ze de meeste last van ondervinden), zo redeneren ze, is vooral een gevaar dat van buiten komt. Als we echter een nadere blik werpen op dit verschijnsel, moeten we concluderen dat het zowel letterlijk als figuurlijk minder vaak 'buiten' het bedrijf gebeurt dan veel bedrijven (ons willen doen) geloven. Letterlijk in de zin dat bijvoorbeeld de trailer- en opleggerdiefstallen (de meest schadevolle diefstallen) in de meeste gevallen niet 'langs de weg' plaatsvinden, maar gewoon vanaf de eigen bedrijfsterreinen. Echter, ook als deze misdrijven wel 'langs de weg' plaatsvinden, of zelfs in een ver buitenland, wil dat niet zeggen dat het automatisch een uitsluitend externe gebeurtenis is.
Private en met name politiële opsporingsinstanties, maar ook opdrachtgevers en verzekeraars (expertisebureaus) kunnen ons in dit verband betere informatie verschaffen. Zo'n beetje alle deskundigen die wij hierover geraadpleegd hebben, rapporteren vergelijkbare ervaringen, namelijk dat grootschalige diefstal van handelsgoederen een vorm van georganiseerde criminaliteit is waarbij heel vaak (sommigen zeggen: altijd) sprake is van enigerlei interne betrokkenheid. Hoe meer ervaring de respondenten hebben met opsporingsonderzoek op dit vlak, des te stelliger zijn ze in hun uitspraak dat van enige vorm van interne betrokkenheid bijna altijd sprake is. Dat interne betrokkenheid in de meeste gevallen aan de orde is, blijkt niet alleen uit opgehelderde zaken, maar ook uit de modus operandi van de delicten zelf: deze verraadt doorgaans kennis van interne processen bij het getroffen bedrijf.
De ervaringen van opsporingsdeskundigen op dit vlak nuanceren dus in belangrijke mate de ervaring van bedrijven dat bij grootschalige ladingdiefstal slechts in een beperkt aantal gevallen sprake is van interne betrokkenheid. Nu moeten we deze ervaringen niet verabsoluteren, omdat ook deze deskundigen een beperkt zicht op het fenomeen (kunnen) hebben. Echter, de bronnen die wij hebben geraadpleegd komen onafhankelijk van elkaar en telkens op basis van eigen ervaringen tot dezelfde conclusie. Dit geeft ons voldoende vertrouwen om aan te nemen dat bij grootschalige ladingdiefstal misschien niet in alle gevallen, maar dan toch op zijn minst in veel gevallen sprake is van interne

betrokkenheid. Dit is een belangrijke aanvulling op de kennis die bedrijven hieromtrent met ons hebben gedeeld.
De wijze waarop interne medewerkers betrokken kunnen zijn, kan variëren van het per ongeluk of opzettelijk verschaffen van informatie aan derden, het fysiek faciliteren van het incident (bijvoorbeeld alarm afzetten), tot aan het zelf plannen en uitvoeren van de diefstal. Dit laatste lijkt bij grootschalige diefstal echter minder aan de orde. Voor de betrokken bedrijven is het irrelevant of een medewerker per ongeluk of opzettelijk heeft meegewerkt aan de totstandkoming van een diefstal; de schade die in beide gevallen wordt veroorzaakt is even groot. We hebben het idee dat veel bedrijven dit risico onvoldoende onderkennen.

Grootschalige diefstal van handelsgoederen is meestal een vorm van georganiseerde criminaliteit. Kennis en aanpak van dit verschijnsel zijn beperkt en verdienen meer aandacht.

Zowel uit de ervaringen van opsporingsdeskundigen als uit de modus operandi van de gepleegde delicten, kan worden afgeleid dat grootschalige ladingdiefstal bijna altijd een vorm van georganiseerde criminaliteit is. Het stelen en verwerken van een aanzienlijke hoeveelheid handelsgoederen vereist een bepaald organisatieniveau en ook logistieke faciliteiten; de goederen moeten immers vervoerd, mogelijk opgeslagen, en weer afgezet worden. De ervaringen die tot nu toe in Nederland zijn opgedaan met de opsporing van daders, laten zien dat het in de meeste gevallen inderdaad om goed georganiseerde criminele netwerken gaat die veelal gebruik maken van kennis uit de bedrijven die ze slachtoffer maken. Daarnaast wordt door deskundigen gesignaleerd dat er ook veel ‘vrijbuiters’ op pad zijn die proberen door middel van bijvoorbeeld het snijden in dekzeilen van vrachtauto’s een ‘graantje mee te pikken’. Hierbij gaat het echter zelden om grootschalige diefstal, maar veeleer om diefstal van kleine hoeveelheden goederen.
De kennis over daders van deze vorm van criminaliteit is beperkt en versnipperd. Wetenschappelijk onderzoek naar deze groep ontbreekt nagenoeg en is gewenst om meer inzicht te krijgen in de risico’s die bedrijven op dit vlak lopen en de wijze waarop ze zich hiertegen kunnen wapenen. Ook de opsporing van daders geschiedt mondjesmaat. De opsporing van deze vorm van criminaliteit vereist een grootschalige en professionele aanpak. Rechercheafdelingen van individuele politieregio’s hebben hiervoor niet de capaciteit en de expertise in huis. Een meer permanente aandacht, bijvoorbeeld op het niveau van het Landelijk Parket en de Nationale Recherche, is naar ons idee gewenst. De omvang en de ernst van het probleem voor de betrokken bedrijven en ook de economische schade die eruit voortvloeit, rechtvaardigen ons inziens deze aandacht. In enkele landen om ons heen (bijvoorbeeld in België en Engeland) staat ladingdiefstal aanzienlijk hoger op de prioriteitenlijst van de politie. Voor een land als Nederland, dat zich graag presenteert als het logistieke knooppunt van Noordwest-Europa, is de huidige politieaandacht voor dit omvangrijke probleem wel erg pover te noemen.

Bedrijven zien handelsgoederen als belangrijkste doelwit van interne criminaliteit

Uit ons onderzoek komt duidelijk naar voren dat vooral de goederenstroom en in mindere mate de gegevensstroom kwetsbaar worden geacht voor interne criminaliteit. Problemen met geld lijken in deze sector van ondergeschikt belang (en spelen met name daar waar nog gewerkt wordt met remboursgelden). Diverse respondenten, zowel bij bedrijven als experts, noemen informatiecriminaliteit een groot risico voor deze sector (gegevens over goederenstroom, klantgegevens en dergelijke). Toch zijn er niet veel incidenten op dit vlak gemeld. Het is niet duidelijk of bedrijven er (nog) geen last van hebben of dat ze deze vorm van criminaliteit niet zo snel ontdekken. We hebben niet het idee dat respondenten onwillig waren om hierover met ons te praten.

Criminaliteit verplaatst zich van loodsen naar ‘buiten’

Sommige experts zien een ontwikkeling waarbij diefstal van handelsgoederen zich heeft verplaatst van de loodsen naar het transport (waaronder grootschalige ladingdiefstallen vanaf het eigen bedrijfsterrein). Volgens hen worden de loodsen in toenemende mate beveiligd en zijn deze moeilijker te kraken. De dieven zoeken nu de zwakkere schakel op: meestal het transport. Op Schiphol bijvoorbeeld is deze verplaatsing in de afgelopen periode ook duidelijk waargenomen. De loodsen van

de grote vrachtafhandelaren aldaar waren jarenlang de plaats waar zeer regelmatig grote hoeveelheden goederen verdwenen. Echter, sinds de invoering van de nieuwe Luchtvaartwet in 2003 zijn deze bedrijven gebonden aan strengere veiligheidsmaatregelen en is het aantal diefstallen gedaald. Tegelijkertijd is echter een toename waar te nemen in diefstallen van handelsgoederen bij bedrijven die op de platforms vliegtuigen laden en lossen. Het toezicht hierop is veel moeilijker te organiseren.

Bedrijven rapporteren niet alle interne criminaliteit

De mate waarin bedrijven geneigd zijn én in staat zijn om interne criminaliteit waar te nemen (en aan de onderzoekers te rapporteren) wordt beperkt door psychologische, cognitieve, economische en juridische factoren.
De *psychologische* factor heeft te maken met veiligheidsbewustzijn. Dit varieert nogal tussen bedrijven. Respondenten in sommige bedrijven zijn geneigd om gebeurtenissen die plaatsvinden buiten de vier muren van het bedrijf automatisch als iets externs te beschouwen, ze leggen geen link met interne bedrijfsprocessen. En hoe groter de fysieke afstand tot het bedrijf, des te 'externer' de gebeurtenis voor hen wordt; een ladingdiefstal in Italië is voor velen externer dan een ladingdiefstal dichtbij huis. Een aardig voorbeeld van deze *mind set* is een respondent die als risico noemde dat bijvoorbeeld bij warm weer de dokdeuren van de loods vaak open blijven, waardoor buitenstaanders binnen kunnen komen. Dat zijn eigen medewerkers daarmee ook een gelegenheid krijgen om spullen van binnen naar buiten te transporteren kwam niet bij hem op. Criminaliteit komt van buiten, zo is de gedachte. In bedrijven waar het veiligheidsbewustzijn daarentegen op een hoger niveau ligt, is men eerder geneigd de mogelijkheid van interne (betrokkenheid bij) criminaliteit te overwegen. Met als gevolg dat deze bedrijven ook vaker interne betrokkenheid waarnemen.
De *cognitieve* factor is dat de kennispositie van bedrijven meestal niet toereikend is om na een incident inzicht te hebben in wat er precies gebeurd is en hoe het gebeurd is. Hier speelt afstand soms wel een rol, maar ook de schaal en de complexiteit van de logistieke keten. Als de lading in bijvoorbeeld Turkije gestolen is, is het voor bedrijven heel lastig om na te gaan wat zich daar precies heeft afgespeeld. Het meest pregnant doet dit probleem zich voor bij luchtvracht, waarbij goederen soms over de hele wereld vliegen. Als aan het einde van de rit blijkt dat er goederen ontbreken, wordt het heel lastig om na te gaan wat er gebeurd is en waar. Toch is kennis heel relevant als het gaat om het vaststellen van interne betrokkenheid. Uit ons onderzoek komt immers naar voren dat hoe méér bedrijven zicht hebben op wat zich heeft afgespeeld, des te vaker ze interne (betrokkenheid bij) criminaliteit vermoeden of aantreffen. Sommige grotere bedrijven die hierop meer zijn ingesteld, kiezen er daarom voor om bij incidenten recherchebureaus in te schakelen.
Als een bedrijf zich bewust is van de mogelijkheid van interne betrokkenheid en kennis heeft van het feit dat hiervan in een concreet geval sprake is, dan kan het toch nog goede redenen hebben om naar buiten toe te doen alsof het van niks weet. Hier komt onder andere de *economische* factor om de hoek kijken; bedrijven hebben er geen belang bij om de buitenwereld op de hoogte te stellen van eventuele interne betrokkenheid bij diefstal, omdat dit voor hen allerlei ongewenste effecten kan hebben. Ze kunnen bijvoorbeeld door de verlader of een andere partij aansprakelijk worden gesteld voor de schade. Mogelijk kunnen ze geen beroep doen op overmacht, zodat ze de gehele schade zelf moeten betalen. Echter, ze kunnen ook imagoschade lijden of klanten verliezen. Strategieën van bedrijven zijn er dan ook op gericht om aansprakelijkheidsstelling te voorkómen. Er kunnen ook *juridische* overwegingen zijn om de zaak binnenskamers te houden. Bijvoorbeeld als de interne criminaliteit is gepleegd door een illegale werkkracht of door iemand van wie de 'papieren' niet in orde zijn of wanneer de arbeidsomstandigheden waarin het delict tot stand kwam niet volgens de regels van de Arbo-wetgeving zijn. Kortom, het bedrijf kan ondanks de geleden schade en de mogelijkheden tot verhaal toch goede redenen hebben om niet naar buiten te komen met incidenten.
Als we deze processen zo bezien, moeten we concluderen dat er zeer waarschijnlijk sprake is van onderrapportage van interne criminaliteit door bedrijven in ons onderzoek. In hoofdstuk 3 hebben we een uitvoerige analyse gemaakt van alle mogelijke onderrapportagebronnen. Hieruit kunnen we afleiden dat onderrapportage een onvermijdelijk fenomeen is in een onderzoek als het onderhavige. We hebben op twee manieren geprobeerd dit verschijnsel te ondervangen. In de eerste plaats door te kiezen voor een definitie van 'interne criminaliteit' die uitgaat van de als problematisch ervaren schade die bedrijven ervan ondervinden. Uit Amerikaans onderzoek onder werknemers blijkt

bijvoorbeeld dat zaken als opzettelijke vernieling, sabotage van werkprocessen, privé-gebruik van bedrijfsmiddelen en dergelijke heel regelmatig vóórkomen. Het feit dat bedrijven in ons onderzoek hiervan naar verhouding weinig melding maken, geeft vooral aan dat ze deze verschijnselen (als ze er al zicht op hebben, wat meestal niet het geval is), niet als problematisch beschouwen voor de bedrijfsvoering. We zagen dat bedrijven dit soort gedrag van hun personeel pas als problematisch gaan beschouwen als het de spuigaten uitloopt of als de schade uitkomt boven een gebruikelijk gemiddelde. In de tweede plaats hebben we getracht het *dark number* terug te brengen door bij opsporingsinstanties aanvullend onderzoek te doen naar de interne betrokkenheid bij criminaliteitsproblemen die de sector zelf als meest schadelijk ervaart: de grootschalige diefstal van handelsgoederen. Uit dit onderzoek kwam naar voren dat hierbij veel vaker dan bedrijven aan ons gemeld hebben, sprake is van interne betrokkenheid. Als het gaat om andere vormen van interne criminaliteit, zoals diefstal/verduistering, corruptie, fraude, handel in illegale goederen of diensten, et cetera, hebben we niet het idee dat we alles boven tafel hebben gekregen, simpelweg omdat bedrijven er vaak zelf geen zicht op hebben en als dat wel het geval is, zijn er weer allerlei mechanismen die ervoor zorgen dat wij als onderzoekers deze zaken niet te weten komen. Het blijft natuurlijk altijd de vraag hoe omvangrijk deze verborgen problemen zijn. Als we echter kijken naar het verloop van de gesprekken in de bedrijven en als we ook rekening houden met onze definitie van interne criminaliteit en het aanvullend onderzoek dat we hebben uitgevoerd, hebben we niet het idee dat er voor de sector *belangrijke* problemen aangaande interne criminaliteit buiten beeld zijn gebleven.

Dé dader van interne criminaliteit bestaat niet

Zowel uit dit onderzoek als uit andere studies komt naar voren dat het heel moeilijk, zo niet onmogelijk is om tot een daderprofiel te komen van personen die zich schuldig maken aan interne criminaliteit. Er worden zoveel persoonlijke en functie- en beroepsgerelateerde achtergrondkenmerken relevant geacht, dat deze hierdoor feitelijk hun relevantie verliezen. De constatering dat er heel veel risicofactoren zijn aan te wijzen, zoals leeftijd, geslacht, aard van het dienstverband, duur van het dienstverband, et cetera, betekent eigenlijk vooral dat iedere werknemer een potentiële dader kan zijn. De conclusie lijkt ons dan ook gerechtvaardigd dat in veel gevallen de gelegenheid van doorslaggevender belang is bij de totstandkoming van interne criminaliteit dan de achtergrond en motivatie van de dader.
Deze conclusie moeten we overigens meteen nuanceren, want vooral bij grootschalige vormen van (interne) criminaliteit zou het zwaartepunt wel eens precies omgekeerd kunnen liggen: hierbij gaat het juist om gemotiveerde daders op zoek naar een geschikt doelwit. Bovendien bleek uit het politie- en justitieonderzoek dat de meerderheid van de verdachten van interne criminaliteit al een strafblad had voordat ze (opnieuw) de fout ingingen. Hieruit kan weliswaar niet worden afgeleid dat veel of zelfs de meeste daders van interne criminaliteit recidiverende criminelen zijn, maar het geeft wel aan dat deze groep op zijn minst ook een significante rol speelt bij dit fenomeen.
Bedrijven zijn in dit verband soms erg gefocust op slechts één of hooguit enkele groepen medewerkers. Zo worden uitzendkrachten door veel bedrijven beschouwd als een risicogroep. Onze analyse laat zien dat dit een te beperkt uitgangspunt is voor succesvolle preventie.

Aard en omvang van interne criminaliteit hangen samen met diverse bedrijfskenmerken

In hoofdstuk 4 hebben we gesproken over factoren op het niveau van bedrijven die gerelateerd zijn aan interne criminaliteit. Het zijn vooral grote bedrijven, bedrijven met risicovolle goederen, bedrijven die zelf het transport uitvoeren en bedrijven die personeelsproblemen hebben die, meer dan andere bedrijven, te maken hebben met interne criminaliteit. Overigens hebben we gezien dat ook de aard van de interne criminaliteit, het soort incidenten, varieert met deze factoren: in grote bedrijven komen bepaalde incidenten bijvoorbeeld veel vaker voor dan in kleine bedrijven.

De complexe logistieke keten werkt criminaliteitsbevorderend

De logistieke keten zelf werkt criminaliteit in de hand. Om te beginnen is het vaak al moeilijk om te ontdekken óf er in een bepaald geval sprake is van criminaliteit. Er gaan grote hoeveelheden goederen

door de bedrijven heen. Als op enig moment de goederen niet zijn waar ze hadden moeten zijn, kan dit allerlei oorzaken hebben; criminaliteit is daar slechts één van. De meeste bedrijven werken bovendien met marges waarbinnen enige schade en verlies is toegestaan. Zolang de vermissingen en de manco's binnen deze marges blijven, voelen bedrijven geen noodzaak om er verder aandacht aan te besteden. Gesteld echter dat het hier wel om interne criminaliteit gaat, welk effect gaat er dan van dit beleid uit op het gedrag van de betrokken medewerkers en hun directe omgeving in het bedrijf? Een remmend effect lijkt ons zeer onwaarschijnlijk. Als duidelijk wordt dat sprake is van een onregelmatigheid (de goederen willen maar niet aankomen bij de klant of de dozen blijken leeg), dan is het vervolgens een hele opgave om na te gaan waar, wanneer en hoe deze is ontstaan. Kortom, de gevolgen van diefstal komen op enig moment wel ergens aan het licht, maar het verschijnsel zelf laat zich vaak veel moeilijker traceren. Een bijkomend probleem is dat bedrijven hier ook niet altijd belang bij hebben, want als blijkt dat het probleem bij hen zit, draaien zij op voor de schade. De complexiteit van de logistieke keten schenkt hen ook de gelegenheid om deze aansprakelijkheid te ontlopen. Het duurt immers vaak enige tijd voordat ontdekt wordt dat er iets mis is, waardoor de sporen en de aanwijzingen al lang en breed verdwenen zijn. Bovendien zijn de goederen in die tijd vaak door zoveel handen gegaan dat onmogelijk kan worden vastgesteld aan welke handen deze goederen zijn blijven 'plakken'. Onderzoek naar de vermissing van de goederen kan zo tijdrovend en kostbaar zijn dat het niet altijd loont om hieraan te beginnen. We roepen in herinnering de logistieke keten rond de luchtvracht: op meerdere continenten onderzoek doen naar de verdwijning van een partij goederen, hoe waardevol ook, loont meestal niet de moeite. Pas als het de spuigaten uitloopt, gaat een dergelijk onderzoek in deze keten lonen.
Kortom, de wijze waarop de logistieke keten functioneert, met zijn vele actoren, de vele overdrachtsmomenten van goederen en de grootschaligheid van het proces, werkt als zodanig criminaliteitsbevorderend.

Preventie van (interne) criminaliteit varieert sterk tussen bedrijven

Bedrijven verrichten, zoals we gezien hebben, wisselende inspanningen om (interne) criminaliteit tegen te gaan. Een kleine groep bedrijven is laag tot zeer laag beveiligd, maar rapporteert naar verhouding ook weinig (interne) criminaliteit. Een hele grote groep bedrijven is middelmatig beveiligd en een kleinere groep is hoog tot zeer hoog beveiligd. De laatste groep bedrijven verricht verregaande inspanningen om (interne) criminaliteit tot een aanvaardbaar niveau te beperken en behoudens enkele uitzonderingen lijken deze bedrijven daar ook aardig in te slagen. De nadruk ligt in alle gevallen op preventie van diefstal van handelsgoederen. Met uitzondering van de hele grote ondernemingen zien we dat heel veel bedrijven hun beveiliging (pas) opschalen naar aanleiding van concrete incidenten die zich hebben voorgedaan.
Er is een patroon waar te nemen in het opschalen van de beveiliging: men begint meestal met bouwkundige en technopreventieve maatregelen. Als deze onvoldoende blijken te werken verlegt men de aandacht meer naar (controle)procedures in het bedrijf. Als ook deze niet het bevredigende resultaat geven (omdat de aandacht telkens verslapt), komt men weer terug bij wat in kleine bedrijven vaak vanzelf gebeurt: informele sociale controle (elkaar aanspreken op normovertredend gedrag, communiceren over gewenst/integer gedrag en dergelijke). Dit is volgens experts ook de meest effectieve strategie, omdat technopreventie, hoe geavanceerd ook, zich altijd laat omzeilen.

De kennis van aanpak en preventie van interne criminaliteit is in een aantal bedrijven gebrekkig. Deze bedrijven maken onvoldoende gebruik van de in de branche aanwezige informatie

Ondanks het feit dat er in de sector behoorlijk veel kennis voorradig is over de preventie en aanpak van -interne- criminaliteit (zie bijvoorbeeld TLN, 2003), is het ons opgevallen dat deze in veel gevallen niet de bedrijven en personen heeft bereikt die wij hebben gesproken. De grote bedrijven zijn over het algemeen wel goed beveiligd en op de hoogte van de risico's die ze lopen. Kleinere bedrijven zijn echter lang niet altijd op de hoogte van de mogelijkheden en (juridische en organisatorische) beperkingen van beveiligingsmaatregelen. Ook de kennis over verzekeringskwesties, bestaande certificeringen en de (on)mogelijkheden van de gang naar de straf- en civiele rechter is bij een aantal bedrijven beperkt. Hierdoor raken deze bedrijven soms gefrustreerd, bijvoorbeeld omdat ze niet

volgens de regels beveiligingscamera's hebben laten ophangen waardoor de beelden van een interne diefstal niet gebruikt mogen worden als grond voor ontslag (waarna de dief mag terugkeren in het bedrijf of schadeloos gesteld moet worden voor het onterechte ontslag).
Bedrijven kunnen zich soms veel geld, moeite en ergernis besparen als ze zich beter zouden informeren over de mogelijkheden tot preventie en aanpak van (interne) criminaliteit. Dit geldt niet alleen voor de wijze waarop ze met een interne verdachte omgaan (zoals in het voornoemde voorbeeld), maar ook voor de screening van nieuw personeel (vindt vaak niet plaats of is gebrekkig), voor de wijze waarop bedrijfsprocedures beter beveiligd kunnen worden, voor de kennis over veilige parkeerplaatsen en voor tal van andere monitoring- en preventiemaatregelen. Bedrijven doen soms erg weinig moeite om kennis te nemen van wat er zoal te koop is op dit gebied. Tekenend hiervoor is de meermalen voorgekomen situatie waarin bedrijven het interview dat wij met ze hadden gebruikten om preventie-ideeën op te doen. Meestal hangt dit gebrek aan aandacht samen met het feit dat beveiliging geen *core business* is en pas aandacht krijgt als de criminaliteitsproblemen een serieuze bedreiging gaan vormen voor het bedrijfsresultaat of voor het imago van het bedrijf.
Omdat van de meeste bedrijven niet verwacht mag worden dat ze zich ontwikkelen tot experts in beveiliging, is bij het proces van kennisoverdracht ondersteuning door externe partijen gewenst. Er zijn verschillende partijen die hierbij een rol zouden kunnen spelen, zoals de brancheorganisaties, maar ook de politie en wellicht ook een organisatie als het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Overigens lijkt het ons in dit verband van groot belang om *pro-actief* te werk te gaan, omdat vooral kleine en middelgrote bedrijven zich vaak niet bewust zijn van de risico's die ze lopen en in die gevallen dus ook niet zelf op zoek gaan naar ondersteuning. Daarnaast zal *herhaling* van de boodschap noodzakelijk zijn om deze bij een deel van de bedrijven 'tussen de oren' te krijgen.

Criminaliteitspreventie staat op gespannen voet met commerciële belangen, maar kan ook een commerciële troef zijn

De grote groep van middelmatig beveiligde bedrijven is in dit verband interessant, omdat we hier bedrijven vinden met de meest uiteenlopende criminaliteitsniveaus. In deze groep bevinden zich veel middelgrote ondernemingen bij wie de beveiliging zich in verschillende stadia van ontwikkeling bevindt: van tamelijk elementair tot tamelijk ontwikkeld. Het lijkt erop dat vooral in deze groep van bedrijven het spanningsveld tussen bedrijfsmatige afwegingen en beveiligingsafwegingen volop speelt. Immers, kleine bedrijven met weinig risicovolle goederen kampen doorgaans niet met serieuze problemen en grote (internationale) ondernemingen met hoog-risicovolle goederen lopen doorgaans voorop als het gaat om nieuwe preventiestrategieën. Als het erom gaat het hoofd boven water te houden, prevaleren de bedrijfsmatige argumenten meestal boven de beveiligingsargumenten. Zeker in de transportsector zijn de marges laag en zullen bedrijfsmatige afwegingen vaker prevaleren. Dit geldt bijvoorbeeld voor veel kleine transportbedrijven die de laatste jaren zijn gegroeid door ook andere logistieke diensten aan te bieden. Daarnaast zien we echter ook bedrijven die het beveiligingsniveau in hun organisatie bewust gebruiken om zich te onderscheiden van concurrenten. Vooral als het gaat om de opslag, het vervoer en de bewerking van dure consumentengoederen, kan het beveiligingsniveau een commerciële troef zijn, omdat verladers en andere opdrachtgevers hierbij een belang hebben. Hierdoor ontstaat een heel divers beeld in de sector; aan de ene kant zien we bedrijven die elektronicaladingen ter waarde van een half miljoen euro vervoeren in huiftrailers die zich eenvoudig laten opensnijden. Aan de andere kant zien we bedrijven die zijn uitgerust met de laatste snufjes en die voortdurend personeel en auto's visiteren, et cetera.

Externe druk stimuleert bedrijven om zich beter te beveiligen

De preventiestrategieën van bedrijven worden niet alleen door bedrijfsinterne factoren beïnvloed, maar ook en vooral door externe factoren. Zo heeft bijvoorbeeld nieuwe wet- en regelgeving in het kader van de terrorismebestrijding (bijvoorbeeld de nieuwe Luchtvaartwet, maar ook de ISPS-code die is ingevoerd in zeehavens) een zichtbaar positief effect op het beveiligingsniveau van de betreffende bedrijven. Door schaalvergroting in de sector ontstaan steeds grotere (groepen van) bedrijven en ook dit heeft een positief effect op de beveiliging, omdat de moederbedrijven doorgaans (hoge) eisen stellen aan de beveiliging van hun dochters. Bovenal zijn het echter de andere actoren in de logistieke

keten die in de huidige situatie, waarin veelvuldig sprake is van grootschalige diefstal van handelsgoederen, een dynamiek creëren die uiteindelijk zal leiden tot verdere opschaling van de beveiliging van bedrijven in deze sector. We spraken eerder over strategieën die bedrijven gebruiken om hun aansprakelijkheid bij diefstal te ontlopen (want ook al zijn alle bedrijven verzekerd, het kost ze bij diefstal altijd een eigen risico en als ze pech hebben veel meer dan dat). Dit leidt doorgaans tot een keten van aansprakelijkheidsstelling, waarbij bijvoorbeeld de klant van de goederen de producent (verlader) aansprakelijk stelt; de verlader stelt de logistiek dienstverlener weer aansprakelijk, die weer de transporteur aansprakelijk stelt, et cetera. Waar het 'rad van avontuur' ook stil blijft staan, er is één zekerheid: er zal altijd één partij in de keten het onderspit delven en schade oplopen. Dit kan de verzekeraar zijn (die moet uitkeren), de verlader (die zijn dure goederen kwijt is en alleen de CMR-waarde terugkrijgt), de logistiek dienstverlener (die contractueel aansprakelijk is maar zich niet kan beroepen op overmacht, omdat het vervoer niet volgens de regels van het contract is uitgevoerd), et cetera.
De partij die het onderspit delft zal, met name als dit vaker gebeurt, strategieën gaan ontwikkelen om dit in de toekomst te voorkómen. Dit fenomeen zien we op dit moment op tal van plaatsen opduiken. Hierbij kan het gaan om verzekeraars die hun premie verhogen en/of strengere voorwaarden stellen aan de beveiliging van logistiek dienstverleners. Ook stellen ze in toenemende mate eisen aan de logistieke contracten die deze bedrijven afsluiten. Verladers volgen een zelfde strategie: ze schroeven hun eisen aan de logistiek dienstverleners op, zodat de kans op diefstal wordt verkleind en de kans op verhaal bij incidenten wordt vergroot. Een initiatief als TAPA is hiervan een voorbeeld. Een andere strategie die verladers in toenemende mate volgen, is dat ze proberen om de transporteurs die hun lading in enig buitenland zijn kwijtgeraakt aansprakelijk te stellen in het land dat hen de meeste mogelijkheden biedt om het betreffende bedrijf voor de volledige schade (dus boven CMR-niveau) aansprakelijk te stellen. Echter ook de logistiek dienstverleners proberen de risico's zoveel mogelijk van hun lijf te houden, bijvoorbeeld door risicovolle lading bij andere bedrijven onder te brengen, door te onderhandelen over wie welke beveiligingsmaatregelen betaalt, et cetera.
Wat we feitelijk zien gebeuren is dat partijen in de logistieke keten hun risico's zoveel mogelijk proberen door te schuiven naar andere partijen in diezelfde keten. Dit gedrag is onmiskenbaar een reactie op het omvangrijke criminaliteitsprobleem zoals hiervoor besproken. Doordat alle actoren in deze keten echter zo afhankelijk van elkaar zijn, kunnen ze niet ontsnappen aan de collectieve gevolgen van het feit dat geleden schade 'in de keten blijft'. Individuele strategieën van bedrijven om zich te onttrekken aan schades of risico's, komen dus uiteindelijk als een boemerang bij hen terug omdat de partijen waarmee ze zaken doen hun schade willen compenseren. Aldus kunnen we concluderen dat de markt in de logistieke keten op dit moment zijn eigen paden zoekt om de omvangrijke schade die wordt geleden door grootschalige diefstal van handelsgoederen op te vangen.

Bedrijven zijn ontevreden over de inspanningen van politie en (in mindere mate) justitie. Verbeteringen op het vlak van voorlichting, communicatie en opsporing zijn gewenst

Heel veel bedrijven zijn niet zo blij met de rol van de politie. De reacties lopen uiteen van apathie tot grote boosheid. De *bottom line* is dat bedrijven zich volstrekt vogelvrij voelen ten aanzien van de criminaliteit waarmee zij te maken hebben. De ergernis heeft betrekking op het doen van aangifte (wordt soms geweigerd, procedure is omslachtig), op de actie die hierop volgt (meestal geen actie) en op de afloop als er wel actie is gevolgd (vaak onbevredigend, zo vinden bedrijven). Het is van belang hierbij op te merken dat respondenten doorgaans wel onderscheid maken tussen de politie als instituut en de politie als concrete personen waarmee ze te maken hebben. Ze zijn vooral ontevreden over het feit dat de politie als instituut zo weinig aandacht voor hen heeft, terwijl ze van tijd tot tijd geconfronteerd worden met slachtofferschap van grootschalige criminaliteit.
We realiseren ons dat klagen over de politie in sommige kringen een soort van tijdverdrijf is, maar in deze sector kunnen we ons wel wat voorstellen bij de onvrede, en niet alleen omdat hij zo algemeen en zo sterk aanwezig is. Als onderzoekers zijn we met grote regelmaat geconfronteerd met min of meer verbazingwekkende ervaringen van bedrijven. Eén zo'n ervaring is bijvoorbeeld dat bedrijven aangifte doen en tegelijkertijd een verdachte aanleveren (met bewijsmateriaal zoals bijvoorbeeld camerabeelden, getuigenverklaringen en soms zelfs een schriftelijke bekentenis van de verdachte). Zeer regelmatig kregen bedrijven in deze gevallen te horen dat de politie geen capaciteit had om ermee

aan de slag te gaan. We hebben dit als onderzoekers ook zelf een keer ervaren tijdens ons bezoek aan één van de opsporingsinstellingen. Op de ochtend dat wij het interview afnamen, had een bedrijf gemeld dat het een verdachte van interne criminaliteit vasthield (de daad -een grootschalige diefstal- was op camerabeelden vastgelegd). De betreffende opsporingsinstantie moest het bedrijf echter melden dat ze geen capaciteit had om iets met deze melding te doen en adviseerde het bedrijf om de verdachte te laten gaan. Een andere ervaring, ook vaak gemeld: een bedrijf wordt slachtoffer van een grootschalige diefstal en lijdt daardoor een grote schade (bijvoorbeeld een half miljoen euro). Er zijn allerlei opsporingsindicaties zoals sporen en dergelijke, maar de politie laat wederom niks van zich horen of meldt dat er geen capaciteit is.
Als we kijken naar de wijze waarop aangiften van interne criminaliteit door politie en justitie worden afgehandeld, zien we in grote lijnen een bevestiging van het beeld dat bedrijven ons tijdens de interviews geschetst hebben: de door de politie opgehelderde interne zaken bestaan voor het overgrote deel uit aangiften waarbij bedrijven zelf de verdachten 'aanleverden'. Zonder deze informatie uit de bedrijven, lost de politie nauwelijks zaken op. Bovendien wordt slechts in een minderheid van de gevallen waarin een aangifte is opgehelderd, overgegaan tot vervolging van verdachten. In de meeste gevallen wordt de zaak geseponeerd (waarbij bedrijven zelf overigens ook een rol spelen). Heel vaak gaat het hierbij zelfs om zaken met verdachten die al een strafblad hebben. Als er al vervolgd wordt bestaat de zwaarste sanctie in tweederde van de gevallen uit een geldboete of een taakstraf. Hiertussen zitten ook zaken met een omvangrijke buit. Wij kunnen ons voorstellen dat deze uitkomsten voor bedrijven uit ons onderzoek erg teleurstellend zijn, ook al kunnen bedrijven zelf ook meer doen om politie en justitie te ondersteunen. Nu doen bedrijven vaak geen aangifte of besluiten ze in een later stadium het strafrechtelijke traject niet te bewandelen, waardoor de opsporing en berechting van daders wordt bemoeilijkt.
De schade die bedrijven ondervinden door grootschalige diefstal van lading kan niet anders dan zeer omvangrijk zijn. Elke dag worden bijna twee trailer/oplegger combinaties gestolen of vrachtwagens met aanhangers (inclusief lading uiteraard). Op jaarbasis ging het in 2003 om circa 630 eenheden (bron: LTT). Hierbij zijn niet inbegrepen alle ladingdiefstallen uit vrachtwagens, waarbij de dieven de oplegger of aanhanger lieten staan, ook niet inbegrepen zijn alle ladingdiefstallen uit loodsen (hiervan bestaat geen centrale registratie). Welke rekenfactor ook wordt gebruikt, men praat snel over enkele honderden miljoenen euro's aan schade per jaar. Dit is een zeer omvangrijk bedrag voor een sector die zo vitaal wordt geacht voor de Nederlandse economie. Als we tegen deze achtergrond kijken naar de politie-inspanningen in Nederland, moeten we concluderen dat deze niet veel voorstellen. Een conclusie die overigens gedeeld wordt door de meeste politierespondenten in ons onderzoek.
Naast meer aandacht voor de opsporing kan er door de politie een wereld worden gewonnen door meer aandacht te hebben voor de criminaliteitsproblemen waarmee deze bedrijven te maken hebben. Waaraan bedrijven in concreto behoefte hebben is een politieapparaat dat hun problemen serieus neemt, dat eventueel voorlichting geeft over preventieve maatregelen en dat hen een toegankelijk aanspreekpunt biedt. Daarnaast wordt breed gepleit voor het 'toegankelijker' maken van de aangifteprocedure. Naar ons idee zou de politie (samen met brancheorganisaties) in dit kader ook moeten streven naar het verhogen van de aangiftebereidheid bij bedrijven. Wat dit laatste punt betreft zijn er overigens wel enige ontwikkelingen gaande. Zo ligt er op dit moment een wetsvoorstel in de Tweede Kamer (wijziging Wetboek van Strafvordering 29 238) dat beoogt de mogelijkheden voor elektronische aangifte te verruimen.

Informatie over grootschalige criminaliteit in de sector is onvolledig en versnipperd. De bestaande informatie kan ook beter benut worden

In oktober 2004 is door overheid en bedrijfsleven het 'Convenant Aanpak Criminaliteit Wegtransport' gesloten. Hierin worden tal van maatregelen genoemd om transportgerelateerde criminaliteit tegen te gaan (NPC, 2004b). In dit convenant wordt onder andere gesproken over het realiseren van meer veilige parkeerplaatsen voor vrachtauto's, over nieuwe opleidingen, over voorlichting, over de inzet van nieuwe technische preventiemiddelen, over het weren van risicovol personeel, over het bevorderen van de aangiftebereidheid bij bedrijven, et cetera.
Ter aanvulling op deze activiteiten pleiten wij ervoor op enigerlei wijze de beschikbare informatie over het probleem te verbeteren en toegankelijk te maken voor betrokken partijen. Wij hebben

geconstateerd dat iedereen in de sector ‘weet’ dat er een groot probleem is op het vlak van de ladingdiefstallen, maar nergens bestaat een betrouwbaar overzicht van hoe dit probleem er nu precies uitziet, hoe vaak zich incidenten voordoen, waar en op welke wijze deze plaatsvinden, wie hierbij mogelijk betrokken zijn, welke ontwikkelingen er zijn, et cetera. Deze kennis is volgens ons van groot belang voor het slagen van tal van andere preventiemaatregelen.
Op dit moment verzamelt het KLPD/LTT gegevens over een bepaald deel van de ladingdiefstallen. Deze informatie is bedoeld voor politiële opsporingsteams. Aangezien er echter niet heel veel opsporingsonderzoeken naar ladingdiefstallen plaatsvinden, wordt deze bron van informatie eigenlijk onderbenut. Het verdient aanbeveling om na te gaan in hoeverre de branche gebruik zou kunnen maken van deze gegevens en op welke manier zij op haar beurt deze gegevens zou kunnen verrijken door nieuwe informatie toe te voegen waarover het KLPD/LTT nu niet beschikt. Ook het Verbond van Verzekeraars heeft kennis die in dit verband toegevoegde waarde kan hebben. Wellicht zou de branche financieel of personeel kunnen participeren in het LTT. Een dergelijke samenwerking heeft ook in Engeland plaatsgevonden en sluit aan bij ontwikkelingen elders in Europa (zoals Eurowatch - uitwisseling van informatie over truckdiefstal op Europees niveau). Door het creëren van een centraal informatiepunt dat wordt gevoed door en ook toegankelijk is voor de betrokken partijen, wordt in ieder geval bereikt dat het probleem inzichtelijker wordt gemaakt, waardoor individuele bedrijven en brancheorganisaties beter in staat zijn om zich te weren tegen nieuwe (criminaliteits)ontwikkelingen.

Summary

Internal Crime in the Logistics Sector

Reason and Objective of the Research

In January 2004 the National Platform for Crime Control (NPC) launched the 'Plan of Action for Safe Entrepreneurship', with as its main target: reducing crime against business by a minimum of 20% by 2008 (NPC, 2004a). To reach this goal a number of projects have been formulated. One of these comprises tackling of internal crime. Another one implies dealing with crime against the transport sector. As a consequence one of the participants in the NPC, the Ministry of Justice, ordered its Research and Documentation Centre (WODC) to conduct a research on internal crime in the logistics sector. In this study the results of this research are described.
This research implies to give insight into the nature and scope of internal crime in the logistics sector in the Netherlands, in particular the internal crime with which logistic services providers are confronted. Subsequently, this study aims to point out which measures are taken by these companies and in what way they react to actual incidents. In this context the role played by police and judiciary is also reviewed. The results of this research aim support the NPC in realising preventive and repressive measures against this form of crime in the logistics sector.

Research Questions

Summarized, the research questions are as follows:

- What is the nature and scope of internal crime against logistic services providers in the Netherlands?
- Which companies are victimized and which characteristics do offenders of internal crime have?
- What measures are taken by companies in the sector to prevent internal crime and how do companies respond to actual incidents?
- In what way are reports of internal crime handled by police and judiciary?

Definition of Internal Crime

We define internal crime as the deliberate violation of standards of behaviour by employees (possibly in cooperation with others), which is aimed against the company for which these employees work (or worked) and which causes or could cause damage that is considered to be problematic to the company.

Research Design

Data on the nature and scope of internal crime in the logistics sector are unavailable in the Netherlands. In addition police and judicial registration systems fail to recognise internal crime as a separate type of crime. To answer the first three research questions we therefore interviewed 139 logistic services providers in the Netherlands, whose core business is warehousing, possibly combined with value added logistics (VAL). By warehousing we mean that goods are not only stored and transferred, but also somehow processed. When processing adds value to the goods, as in assembly, repairs, and other minor industrial activities, one speaks of VAL. An administrative overview of this selection of companies does not exist. Companies have therefore been selected by means of various membership lists of representative organizations and other logistic services umbrella organizations.

This way we found 353 (unique) companies of which 285 satisfied our conditions. Of these, 139 (49%) participated in an interview, generally carried out by the person within the company the most knowledgeable in security matters. As far as we have been able to ascertain the selected companies form a representative sample of the sector
In addition to the companies fifteen experts were also interviewed in order to prepare the questionnaire and to validate and complete the data. The experts were private and police experts on criminal investigation, risk consultants, insurance specialists, clients of logistic services providers, and policy advisors of representative organizations in logistics.
To answer the final research question, we approached all regional police forces in the Netherlands with branches of the participating companies in their districts. We asked them which of the companies had reported cases of crime to the police between January 2002 and December 2004 and, if so, which characteristics these reports of crime had and whether the reported crimes had been solved. Subsequently, the collected data from police were completed with the data provided by the company interviews. At the Central Criminal Records Office in Almelo we investigated whether suspects of these crimes had been convicted, and if so, which sentences had been imposed.

Short Description of the Studied Companies

Almost all interviewed companies were internationally oriented and over half of them were involved with goods which from a theft point of view can be characterized as high-risk. The companies varied in size: over one quarter of the companies had less than fifty employees while the rest of the companies was medium sized or big (which means fifty to two hundred employees or over two hundred employees). Almost two thirds of the companies was not actively involved in the actual transport of those goods or mainly used subcontractors to take care of the transport for them. The companies under study were geographically concentrated in several regions of the Netherlands like Schiphol, Rotterdam (harbour and agglomeration), Noord-Brabant (mainly Moerdijk, Tilburg, and Eindhoven), and Limburg (mainly Venlo).

Main Findings

Nature and Size of Reported Internal Crime

Companies perceived a bigger problem in external crime than in internal crime. Almost half of the companies (48%) identified internal crime as a problem they encountered every now and then or more regularly, while 18% identified internal crime as a serious problem. Most companies (87%) had been victim of some sort of internal crime at least once between 2002 and 2004. On average, companies reported eleven incidents in the past three years. Half of the victimized companies reported less than five incidents. Most companies (61%) reported victimization of some sort of embezzlement. Embezzlement was also the type of crime the highest number of reported incidents. Generally, this concerned smaller forms of embezzlement like warehouse personnel taking away one commodity or one box of commodities. However, the embezzlement of larger amounts of high value goods was also regularly reported.
Of the companies 34% reported being victim of some sort of burglary with supposed or clear internal involvement. Burglary not only takes the form of warehouse and office building burglary, but often of vehicle burglary (cargo theft). More often than in the cases of embezzlement, this involves large-scale incidents with severe damage to companies. The larger the scale of theft the greater the chance of external involvement.
Of the companies 29% reported being victimized by employees' unprofessional behaviour or negligence. In most cases this misconduct was all about neglecting to follow standardized (safety) procedures resulting in circumstances in which different forms of crime could take place (often burglary or embezzlement of large amounts of goods).
Of the companies 17% reported having dealt with verbal or physical violence between colleagues. A comparable number of companies reported experience with cases of fraud. Fraud can be clearly

divided into small-scale and large-scale fraud. Small-scale fraud, mostly reported, concerns fiddling with expense claims, writing too many hours and fiddling with waybills. Large-scale fraud deals mostly with managers or employees in specialist (financial) functions who use their powers and freedom to benefit themselves. On average, of all types of crime fraud shows to bring the highest damage to companies.
Of the companies 11% reported being victim of employees using company assets for private purposes. A comparable number of companies reported sensitive company information to have been leaked to rival companies by employees. Often, this last category involved ex-employees who had left the company with some sort of disagreement and found employment within rival companies.
In addition, we discussed several other forms of crime, which were all reported by less than 10% of the companies. Sabotage of industrial processes (9% reports victimization), vandalism (8%), (internal involvement in) robberies as well as corruption (both 5%), conning, illegal trade, and employees using company assets for personal commercial activities (all 3%).
Most forms of crime are confronted with are somehow transport related. Companies view these forms of crime (robberies, theft of vehicles, and theft from vehicles) as the most important crime problem they encounter in their sector. Of all incidents (external and internal), burglary (including vehicle and cargo theft) was reported most often: 77% of the companies was at least once victim of such crime in the last three years. Of all incidents of burglary which were reported, in only 14% internal involvement was suspected.

Dark number

The above-mentioned findings are based on reports by the companies themselves. We know however, that there are several underreporting effects which lead to not all internal incidents being reported. Internal incidents like fraud and illegal trade can remain hidden within the company because they leave no or little trace. Embezzlement is regularly discovered, for example in case of missing goods, but is sometimes difficult to explain (embezzlement is only one of many possible explanations for missing goods). Furthermore, companies do not always have interest in labelling missing goods as embezzlement, because they risk being held responsible by the owner of the goods or damaging their image. However, some companies are hardly aware of the fact that missing goods may have to do with internal crime. Reported embezzlement therefore forms the tip of the iceberg. Incidents may be uncovered, but companies are not always capable of identifying internal involvement or prepared to judge this as such. This mainly concerns transport related crime (robberies, burglary, and large-scale cargo theft). The identification of internal involvement turns out to be related to security awareness and knowledge: the higher the security-awareness within companies and the more knowledge is available about facts and circumstances surrounding incidents, the more often companies are able to suspect or point out internal involvement. For several reasons respondents might have had limited knowledge of the actual circumstances surrounding incidents. For example, some may have been in function for only a small period of time, some may only have had information on one or a limited number of branches of the company, or some may only have had knowledge of certain forms of crime. In those cases where respondents did have complete knowledge, they may not always have been willing to talk about it, because of commercial considerations or various personal motives.
Additional research into various forms of transport related crime brought to light that there is serious evidence that internal involvement is much more common than companies believe or want us to believe. According to all interviewed experts, especially in the case of large-scale cargo theft (from or out of vehicles and warehouses) in most cases (some experts say: in all cases) internal knowledge is used in one way or another. This image differs strongly from the one given by the companies. We therefore conclude that in many cases where companies speak of external crime internal knowledge will have been used.

Characteristics of Companies Victimized by Internal Crime

The characteristics of the victimized companies that are most strongly related to the prevalence and frequency of internal crime are the following:

- The *size* of the company (the bigger the more crime);
- Problems related to the *recruitment* of personnel (with prevalence more crime);
- The nature of *business activities* (the more transport related the more crime);
- The presence of high-risk *goods* (if present more crime).

Furthermore, characteristics like the level of security and the presence of external personnel are also related to the level of internal crime. However, these relations disappear when we account for the above-mentioned factors. The link between the level of security and the scope of internal crime is a difficult one as many companies upscale their levels of security following incidents that take place. Instead of a negative correlation, we therefore find a positive correlation: better secured companies report more internal crime. This however does not mean that preventive measures fail to have effect on the reduction of internal crime. Within the framework of this research the precise effect is hard to determine. Striking is furthermore that companies in Rotterdam report significantly less (internal) crime than companies in other regions do. This difference can partly be explained by the fact that the companies under investigation in this region are relatively small and have no transport facilities. However, even when we take this effect into account, companies in Rotterdam seem to report less crime then comparable companies in other parts of the country. Our research data do not offer any specific leads to explain this difference.
Finally, we have to acknowledge that some forms of (internal) crime are much more sensitive to differences in the above-mentioned company characteristics than others. The level of embezzlement, vandalism or fraud usually varies stronger with these characteristics than, for example, the level of burglary. As far as burglary is concerned, differences between companies are usually much smaller: all companies seem to face the same problems in this respect.

Characteristics of Offenders of Internal Crime

Companies identified various characteristics when it comes to the background of persons that have ever been suspected of some form of internal crime. Respondents mentioned personal problems (monetary as well as social problems like addiction and divorce), demographic characteristics (unskilled young males, sometimes of immigrant origin), personality characteristics (underdeveloped moral standards, living beyond one's means, reckless or kicking behaviour), and a criminal past or people involved in a criminal subculture or network. Also when it comes to the relation these persons have to the company various diverting characteristics were mentioned. Although in this respect temporary workers were often cited, in almost as many cases offenders turned out to have had a long history within the company. In most cases they worked in the warehouse (mainly shop-floor workers, but in some cases also supervising or controlling personnel). Furthermore, specialists as well as managers were cited). Finally, conflicts over various subjects were mentioned to be related to the incidence of committed crimes.
All these characteristics are somehow related to the occurrence of internal crime. This relation may however differ largely for different forms of crime as for example personnel leaking sensitive information to rival companies shows to have more specific characteristics than offenders of embezzlement. Respondents with only limited experience with internal crime often stated that they were very surprised about the offenders (hard workers, loyal to the company, long history with the company, never any troubles, et cetera). Respondents with more experience with internal suspects mentioned not to be able to point out specific standardized characteristics as the backgrounds of these offenders turned out to differ too much. Combining these answers with the fact that the remaining respondents cited various characteristics, we are inclined to conclude that the personal and professional backgrounds of offenders of internal crime are less important than situational factors. This does not imply that some employees (based on their criminal backgrounds) do pose a serious threat. It would however be wrong to think of these employees as the only high-risk group.

Taking Preventive Measures

It is difficult to separate preventive measures against internal crime from those against external crime. In many companies this distinction did not exist. Only a small number of companies was lowly

secured. Generally, these companies were small and dealt exclusively with low-risk goods. On average, most companies in the logistics sector take a range of preventive measures to fight (internal) crime. In the large group of moderately secured companies, several preventive measures were taken. These were mainly constructional and technological measures (entry protection with fences, camera surveillance, detection and alarm devices, et cetera). A smaller group of (mainly large) companies was highly secured. In addition to the above-mentioned measures we found these companies to take various forms of monitoring measures like controls on in- and outgoing people and goods through visitation, extensive screening of new personnel, et cetera.
There seems to be an order in the preventive measures that more and less secured companies do take: the least secured companies start with constructional and techno preventive measures, while better secured companies emphasize on (controlling) all kinds of company procedures. However as the attention given to these procedures often weakens in time (and because these procedures may conflict with commercial interests), the best secured companies focus their attention on the use of social control mechanisms (which is imposed more or less automatically in smaller companies). The larger the company, the more it deals with high-risk goods, and the more extensive the processing of these goods, the higher seems to be the level of security.
Within most companies, the emphasis on security lies in preventing theft of commodities. Most companies identified this as their biggest threat. A number of companies also mentioned the vital importance of their information systems. Theft of money is of smaller risk for most companies (except for those working with cash on delivery parcels). Although over half of the companies stated that policies against fraud form an integral part of their management procedures, we did not get the idea that fraud (as in forging/manipulation of documents, et cetera) got any serious attention.
Companies had varying ideas of the effectiveness of the various preventive measures. These depended mainly on the above-mentioned stages of security in which they found themselves: companies which had just placed a fence around their business premises were usually very positive regarding its preventive effects. The same holds for companies which only recently had installed surveillance cameras. In the highly secured companies respondents were usually content with visitation procedures although in some of these companies, respondents already mentioned its shortcomings, while pointing out that additional social control mechanisms should be used as techno preventive measures and control mechanisms always may be evaded.
With the exception of a number of large, well secured companies, we found that many companies take their preventive measures in response to incidents with which they are confronted. Financial restrictions are important here as many respondents mention financial limitations as an important obstacle in taking preventive measures. Only if all else fails, expensive measures will be taken. Pressure from external groups (clients, insurance companies, et cetera) may play an important role in this respect. Other obstacles which companies experienced follow from legal or organizational grounds. As for legal limitations, this mainly concerns problems around privacy legislation (for example when placing camera surveillance systems or imposing visitation procedures). Furthermore, companies mentioned employee resistance against various forms of control mechanisms. This however, was mainly an issue in smaller companies.

Company Responses to Actual Incidents of Internal Crime

Above, we already mentioned that with the exception of some larger companies, many companies responded to incidents by adjusting their preventive measures or organizational procedures. Furthermore, we found that the responses to actual incidents strongly depended on the sort of incident and its circumstances. In case of embezzlement for example, companies were more likely inclined to conduct internal research than in case of burglary (with internal involvement). In case of 'internal' burglary however, companies were much more likely to report this crime to the police than embezzlement. Fraud was only reported in few occasions. Private investigators were only called in when there was a certain level of damage. On average, we can conclude that the higher the damage of the incident, the more measures are taken.
Company responses to offenders of internal crime were more homogeneous. In almost all cases that involved internal employees, these employees were dismissed or urged to resign 'voluntarily' (while threatening to report the crime to the police). In case of less serious forms of violation of standards of

behaviour such as negligence, a warning may be given or a remark may be made in the employee's personal file. Calling in the judiciary (a criminal judge or a civil judge to recover the damage from the offender) was only reported in very few occasions. Especially some larger companies seemed to have this as a standardized policy. Many companies however, had serious complaints about the fact that civil actions usually are very unsuccessful while being very costly as well as time-consuming. A number of companies is pronouncedly frustrated by the procedures of dismissal when confronted with the civil judge as their reasons for dismissal were found to be insufficient (the evidence was inadmissible or lacking). Even worse, in some cases they were forced to compensate the offender and/or rehire him. This problem restrains many companies from calling in a civil judge. They much rather try to reach a mutual agreement with the offender to compensate the damage that has been done. Concerning the reporting of crimes to the police, we found that some (usually larger) companies had this as a standardized policy. However, most companies only reported to the police when they were forced to do so (as imposed by the insurance company) or when they had a clear suspect they want to get rid of. When there was no internal or external need to report the crime to the police, by far most companies preferred to deal with the incident internally.

The Handling of Reports of Crime by Police and Judiciary

If we look at the way in which reports of internal crime are handled by police and judiciary, generally we find a confirmation of the view that was given by the companies: those internal crimes that have been solved were almost exclusively those where the companies themselves handed over actual suspects. Without information from the companies, the police is only seldom capable of solving the crime. Furthermore, only in a limited number of cases in which a crime is solved, legal actions are taken. In many occasions cases were dropped, even in those instances where suspects already had a criminal record. When a conviction did follow, in two thirds of the cases the severest sanction consisted of a fine or a task penalty.
Many companies will find these conclusions confirm their view that police and judiciary fail to do their duty in preventing crime against business. However, companies themselves also have to take responsibility when it comes to prosecuting crime. Often companies refrain from reporting crimes to the police or withdraw their report later on because they prefer to deal with the case internally or prefer to call in a civil judge. This further diminishes the possibilities for police and judiciary to trace suspects and bring them to trial.

Final Conclusion

We can state that the logistic services sector is vulnerable to (serious types of) crime, as is evidenced by the nature and scope of the incidents which were reported by the companies. More often than is assumed by companies, internal involvement is found when crime takes place. Experiences from various knowledgeable (criminal investigation) experts point in this direction. The companies themselves, as well as representative organizations, police and judiciary can contribute significantly to reduce this problem to an acceptable level.

Geraadpleegde literatuur

AIC (Australian Institute of Criminology)
Crimes against Business; a review of victimization, predictors and prevention, Canberra, AIC, 2004
Atkinson, K.
How to protect your goods from theft, *Logistics Management and distribution Report*, nr. 3 (zie http://www.manufacturing.net/lm/index.asp?layout=articleWebzine&stt=001&articleid=CA68557&pubdate=03/01/01)
BCC (British Chambers of Commerce)
Setting business free from crime; a crime against business survey by the British Chambers of Commerce, Londen, BBC, 2004
Brown, R.
The nature and extent of heavy goods vehicle theft, Londen, Home Office Police Research Group, 1995
Cohen, L.E., M. Felson
Social Change and Crime Rate Trends: A Routine Activity Approach, *American Sociological Review*, 44, 1979, pp. 588-608
Cools, M.
Werknemerscriminaliteit; criminaliteit tegen bedrijfsactiva; strafbare gedragingen gepleegd door werknemers in grote bedrijven, Brussel, VUPress, 1994
Cools, M.
Werknemersfraude, in: R.N.J. Kamerling, M. Pheijffer (red.), *Vijftien over fraude*, Amsterdam, NIVRA, 1999, VERA-publicatiereeks, nr. 7
Dijk, T. van, H. Elffers, D.J. Hessing, A.B. Hoogenboom
Bewust van de gevaren van criminaliteit, Rotterdam/Arnhem, Sanders Instituut - EUR/Gouda Quint, 1999
Eggen, A.T.J., M. Kruissink, P. van Panhuis, M. Blom
Criminaliteit en opsporing, in: W. van der Heide, A.T.J. Eggen (red.), *Criminaliteit en rechtshandhaving 2003*, Den Haag, Boom Juridische uitgevers/CBS/WODC, 2005
Elzinga, A., P. Klerks
Interne criminaliteit; Kenmerken en mogelijkheden voor een aanpak, Den Haag, Ministerie van Justitie, directie PJS, 1998
EVO
Veiligheid en beveiliging onder de loep: voorkomen van fraude en criminaliteit in de logistiek, Zoetermeer, EVO, 2004
Fijnaut, C.J.C.F., F. Bovenkerk, G.J.N. Bruinsma, H.G. van de Bunt
Inzake opsporing; enquêtecommissie opsporingsmethoden; bijlage 9 - deelonderzoek 2: De branche van het wegtransport, Den Haag, SDU, 1995
Giacalone, R.A., J. Greenberg (red.)
Antisocial Behavior in Organizations, Thousand Oaks, California [etc.], Sage, 1997
Giacalone, R.A., C.A. Riordan, P. Rosenfeld
Employee sabotage: toward a practitioner-scholar understanding, in: R.A. Giacalone, J. Greenberg (red.), *Antisocial Behavior in Organizations*, Thousand Oaks, California [etc.], Sage, 1997, pp. 109-129
Green, G.S.
Occupational Crime, Chicago, Nelson-Hall, 1990
Greenberg, J.
The STEAL motive: managing the social determinants of employee theft, in: R.A. Giacalone, J. Greenberg (red.), *Antisocial Behavior in Organizations*, Thousand Oaks, California [etc.], Sage, 1997, pp. 85-108
Heuvel, G.A.A.J. van den
Werknemersfraude, een beknopte terreinverkenning, in: H. de Doelder, A.B. Hoogenboom (red.), *Witteboordencriminaliteit in Nederland*, Deventer, Gouda Quint,1997, pp. 151

Hoekema, A.J.
Rechtsnormen en sociale feiten; een sociologisch onderzoek naar repressieve reacties op kleine havendiefstal, Rotterdam, Universitaire Pers Rotterdam, 1972
Hoffmann
Hoffmann Statistiek, Almere, Hoffmann Bedrijfsrecherche BV, 2000-2004
Hollinger, R.C., J.P. Clark
Formal and informal social controls of employee deviance, *Sociological Quarterly*, 23, 1982, pp. 333-343
Huiras, J., C. Uggen, B. McMorris
Career jobs, survival jobs and employee deviance: a social investment model of workplace misconduct, *Sociological Quarterly*, 41(2), 2000, pp. 245-263
Jensen, G.F., R. Hodson
Synergies in the Study of Crime and Workplace, *Work & Occupations*, 26(1), 1999, pp. 621
Krause, M.S.
Contemporary white collar crime research: a survey of findings relevant to personnel security research and practice, 2002 (The personnel security managers' research program) (zie www.navysecurity.navy.mil/white%20collar%20crime.pdf)
Mars, G.
Occupational Crime, Ashgate/Dartmouth, Aldershot [etc.], 2001
Mayhew, C.
The detection and prevention of cargo theft, Canberra, AIC, 2001, Trends and issues in crime and criminal justice, nr. 214
McKinnon, I., F. Heinrich-Jones
Fighting lorry load theft - a partnership approach, 2000, september (Paper presented at the IUMI Conference / Cargo Workshop)
Murphy, K.R.
Honesty in the Workplace, Pacific Grove, California, Brooks/Cole, 1993
Niehoff, B.P., R.J. Paul
Causes of Employee Theft and Strategies that HR Managers can use for Prevention, *Human Resource Management*, 89(1), 2000, pp. 51-65
NIPO
Slachtofferschap criminaliteit bij bedrijven en instellingen; Monitor Bedrijven en Instellingen: nulmeting onder 5.000 vestigingen, Amsterdam, NIPO, 2002
NPC (Nationaal Platform Criminaliteitsbeheersing)
Actieplan Veilig Ondernemen, Den Haag, NPC, 2004a
NPC (Nationaal Platform Criminaliteitsbeheersing)
Convenant Aanpak Criminaliteit Wegtransport, Den Haag, NPC, 2004b
PWC (PricewaterhouseCoopers)
Economic Crime survey 2003, Amsterdam, PWC, 2003
Robinson, S.L., J. Greenberg
Employees behaving badly; dimensions, determinants and dilemmas in the study of workplace deviance, in: C.L. Cooper, D.M. Rousseau (red.), *Trends in Organizational Behavior*, New York, John Wiley & Sons Ltd, 1998, jrg. 5, pp. 1-30
TLN (Transport en Logistiek Nederland)
Succesvol Risicomanagement, Zoetermeer, TLN, 2003
Traub, S.H.
Battling Employee Crime; A Review of Corporate Strategies and Programs, *Crime & Delinquency*, 42(2), 1996, pp. 244-257
TrendMeter
Criminaliteit blijft hoog; ondernemers doen minder aangifte, *Forum - Opinieblad van VNO/NCW*, 2000
VNO-NCW
Ondernemers zijn het zat! Politie laat criminaliteit tegen bedrijven links liggen, *Forum - Opinieblad van VNO/NCW*, 2003
Wielenga, A.

Fraude de baas; een handleiding voor de beheersing van interne criminaliteit, Alphen aan den Rijn/Zaventem, Samson, 1992

Bijlage 1 Vragenlijst deel 1: Standaard vragenlijst logistiek dienstverleners

Introductie

Hartelijk dank voor de tijd die u voor mij heeft vrij gemaakt (visitekaartjes uitwisselen). Ik zal me eerst even aan u voorstellen. Ik ben … en werk als onderzoeker voor het Bureau voor Toegepast Veiligheidsonderzoek. Zoals u hopelijk al in de aanbevelingsbrief heeft kunnen lezen doen wij in opdracht van het Ministerie van Justitie en met medewerking van TLN, NDL, Fenex, EVO en KNV een onderzoek naar interne normovertredingen en interne criminaliteit. Specifiek doen wij dit onder logistiek dienstverleners voor wie warehousing *en/of* value added logistics *een kernactiviteit is. Het onderzoek moet leiden tot betere preventieve en repressieve maatregelen vanuit de overheid en de brancheorganisaties om bedrijven te helpen de kosten van deze schadepost te verkleinen. Voor de brancheorganisaties geldt dat zij de resultaten van dit onderzoek weer kunnen gebruiken om beleidsmaatregelen te beïnvloeden. Om goed op de knelpunten die de bedrijven ondervinden in te spelen is het nodig een zo exact mogelijk beeld te krijgen van alle bedrijven die op dit gebied actief zijn, de problemen die zij ondervinden en de maatregelen die zij nemen om schade te voorkómen. We hebben dan ook een groot aantal bedrijven geselecteerd om aan dit onderzoek mee te doen. Ik zal u het komend anderhalf uur in verschillende blokken uiteenlopende vragen stellen. In ruil hiervoor ontvangt u van ons t.z.t. natuurlijk het onderzoeksrapport en tevens een door ons samengestelde* reader *met daarin voor u interessante artikelen over interne criminaliteit.*
Ik realiseer me dat het bij het beantwoorden van de vragen in bepaalde gevallen kan gaan om gevoelige bedrijfsinformatie waar u liever niet met buitenstaanders over praat. Ik wijs u er op dat alle door u verstrekte gegevens zéér vertrouwelijk worden behandeld. Wij zullen op geen enkele wijze gegevens openbaar maken waarin uw bedrijf herkenbaar naar voren komt. Bovendien zijn wij als onderzoekers ook niet geïnteresseerd in het soort kennis waarmee potentiële daders in de toekomst mogelijk hun slag kunnen slaan of waarmee mogelijke concurrenten u kunnen benadelen. Ten slotte geef ik u in overweging dat een adequate aanpak van problemen, bijvoorbeeld op brancheniveau, pas mogelijk is wanneer er een zo volledig mogelijk beeld bestaat van wat er nu eigenlijk in de diverse bedrijven speelt. Ik wil u daarom van harte uitnodigen de volgende vragen zo volledig mogelijk te beantwoorden. Als u om welke reden ook een bepaalde vraag toch liever niet beantwoordt, geeft u dit dan a.u.b. even aan.

1 Algemeen (achtergrond)

1.1 Datum interview
___ / ___ / _____

1.2 Interviewer
1 Ben Rovers
2 Edo de Vries Robbé
3 Karin van Wingerde

1.3 Aanduiding bedrijf (met code)
_____

1.4 Aanvangstijd interview
___ : ___

1.5 Eventueel andere noodzakelijke informatie

2 Algemene gegevens

Eerst zou ik graag wat algemene gegevens willen verzamelen. Daarvoor stel ik u een aantal vragen.

2.1 Functie - Wat is uw functie binnen het bedrijf?

1 *Security* Manager
2 Kwaliteitsmanager
3 Directeur
4 Hoofd Personeelszaken
5 *Operations* Manager
6 Logistiek Manager
7 *Facility* Manager
8 Anders, nl:

2.2 Lengte dienstverband - Hoe lang bekleedt u deze functie al?

1 Weet niet/wil niet zeggen
2 ____ jaar

2.3 Tijd aan *security* - Hoeveel van uw tijd bent u bezig met *security* aangelegenheden?

1 Weet niet/wil niet zeggen
2 Full time
3 20 tot 30 uur per week
4 10 tot 20 uur per week
5 Minder dan 10 uur per week
6 Anders, nl:

2.4 Ander *security* personeel - Als er naast u binnen uw bedrijf nog andere personen met het thema s*ecurity* belast zijn, kunt u dan aangeven wat voor functie zij hebben en hoeveel uren (incl. eventuele ondersteuning) zij hieraan besteden?

1 Geen anderen
2 *Security* afdeling
3 Kwaliteitsbeheer
4 Afdeling personeelszaken
5 Interne accountant(sdienst)
6 *Compliance* afdeling
7 Andere functionarissen, nl:

2.5 Communicatie met management (Alleen indien respondent geen leidinggevende is) - Hoe verloopt de communicatie over het thema *security* met het management?

1 Rechtstreeks
2 Schriftelijk
3 Indirect via:
4 Alleen in speciale gevallen, nl:
5 Anders, nl:

2.6 Achtergrond - Wat is uw achtergrond qua opleiding en vorige werkkring?

Hoogst genoten opleiding:

1 Weet niet/wil niet zeggen
2 Mavo/lbo niveau, nl:
3 Havo/mbo niveau, nl:
4 Vwo-niveau
5 Hbo-niveau, nl:
6 WO-niveau, nl:
7 Anders, nl:

Vorige werkkring (combinaties mogelijk):

1 Weet niet/wil niet zeggen
2 Logistiek
3 Beveiliging
4 Politie
5 Management
6 Anders, nl:

2.7 Aard onderneming - Wat is de aard van de onderneming? Is dit…?
1 Weet niet/wil niet zeggen
2 Holding met _____ werkmaatschappijen
3 Werkmaatschappij
4 Zelfstandige onderneming
5 Anders, nl:

2.8 Schaal onderneming - Op welke schaal opereert het bedrijf?
1 Weet niet/wil niet zeggen
2 Regionaal
3 Nationaal
4 Internationaal
5 Nationaal en internationaal

2.9 Aantal vestigingen en warehouses - Hoeveel vestigingslocaties en en/of *warehouses* heeft uw bedrijf?
1 Weet niet/wil niet zeggen
2 _____ vestigingslocaties in Nederland
3 _____ w*arehouses* in Nederland
4 _____ vestigingslocaties in het buitenland
5 _____ w*arehouses* in het buitenland

2.10 Werkgebied - Is uw werkgebied hetzelfde als dat van de onderneming? Zo nee, kunt u aangeven hoeveel vestigingslocaties en/of werkmaatschappijen er onder uw bevoegdheid vallen?
1 Weet niet/wil niet zeggen
2 Ja, werkgebied is hetzelfde
3 Nee, _____ Werkmaatschappij(en)
_____ Vestigingslocaties in Nederland
_____ Vestigingslocaties in het buitenland

2.11 Locatie en uitleg - Kunt u per vestigingslocatie in Nederland aangeven hoeveel *warehouses* zich er bevinden, in welke geografische regio ze liggen en of ze onder uw verantwoordelijkheid vallen (Int: gebruik de volgende codes: a=Schiphol, b=Rotterdam, c=overig Randstad, d=Noord-Brabant/Limburg en e=anders)?
1 Weet niet/wil niet zeggen
2 Locatie 1: ___ *warehouses*, _____, _____
3 Locatie 2: ___ *warehouses*, _____, _____
4 Locatie 3: ___ *warehouses*, _____, _____
5 Locatie 4: ___ *warehouses*, _____, _____
6 Locatie 5: ___ *warehouses*, _____, _____
7 Locatie 6: ___ *warehouses*, _____, _____

2.12 Kernactiviteiten - Wat zijn voor uw bedrijf de kernactiviteiten (meerder antwoorden mogelijk) en kunt u per activiteit aangeven welk aandeel in de werkgelegenheid zij hebben?
1 Weet niet/wil niet zeggen
2 Transport
3 Opslag en overslag
4 *Value Added Logistics*

5 *Value Added Services* (bijvoorbeeld douaneafhandeling of klantenservice)
6 Post- en koeriersdiensten
7 Anders, nl:

2.13 Bewerkingen - Kunt u van de *warehousing* en de *value added logistics* activiteiten aangeven wat voor uw bedrijf de drie belangrijkste bewerkingen zijn die worden toegepast op de producten (Int: geef met 1, 2 en 3 aan welke productgroepen het belangrijkst zijn)?
1 Weet niet/wil niet zeggen
2 Labellen/Stickeren
3 Verpakken
4 Groupage
5 Handleidingen toevoegen
6 Assemblage
7 Orderverzameling/Orderpicking
8 Opslag en overslag
9 Testen/Kwaliteitscontrole
10 Retourname
11 Anders, nl:

2.14 Productgroepen - Wat zijn de drie belangrijkste productgroepen die door uw bedrijf worden bewerkt (Int: geef met cijfers aan welke productgroepen het belangrijkst zijn)?
1 Weet niet/wil niet zeggen
2 Elektronica/Hightech
3 Kleding/Schoenen
4 Farmacie
5 Levensmiddelen (*food*)
6 *Non-food*
7 Witgoed
8 *Automotive* (auto-industrie)
9 Woningtextiel
10 Kantoorartikelen
11 *Spare parts* (reserve onderdelen)
12 Doe het zelf
13 Papier
14 Boeken/Multimedia
15 Chemie
16 Bouw
17 Industriële producten
18 Overig, nl:

2.15 Personeel in dienst - Kunt u mij zeggen hoeveel personen er op dit moment bij uw bedrijf in totaal in Nederland en eventueel ook in het buitenland werkzaam zijn (Int: bij een schatting gemiddelde van twee uitersten nemen)?
1 Weet niet/wil niet zeggen
2 Totaal: _____
3 Nederland: _____

2.16 Eigen/extern personeel - Als ik op een willekeurige dag bij uw bedrijf zou tellen hoeveel mensen er op en rond uw bedrijf aan het werk zijn, hoeveel zijn dit er dan en hoeveel van hen zijn er dan niet vast bij u in dienst, maar werken voor andere bedrijven? Kunt u ook aangeven wat dit voor soort mensen zijn?
1 Weet niet/wil niet zeggen
2 In totaal _____, waarvan _____ NIET in vaste dienst, nl:

2.17 Problemen werving personeel - Heeft uw bedrijf wel eens moeite met het werven van goed personeel? Zo ja, voor welk(e) functieniveau(s) geldt dit dan en kunt u een korte toelichting geven?

1 Weet niet/wil niet zeggen
2 Nee
3 Ja, problemen met het vinden van _____ omdat:

2.18 Verloop personeel - Hoe groot (op een schaal van zeer gering tot zeer groot) is gemiddeld genomen het verloop onder uw personeel en voor welk functieniveau is dit het grootst?

1 Weet niet/wil niet zeggen
2 Zeer gering
3 Gering
4 Regelmatig
5 Groot
6 Zeer groot

Verloop het grootst voor:

1 Werkvloer, nl:
2 Kaderpersoneel, nl:
3 Anders, nl:

2.19 Uitbestede bedrijfsactiviteiten - Kunt u aangeven welk van de volgende en eventueel andere bedrijfsactiviteiten op uw bedrijf deels of geheel zijn uitbesteed aan andere bedrijven?

1 Weet niet/wil niet zeggen
2 Fysieke transport
3 Onderhoud computernetwerk
4 Schoonmaak
5 Financiële administratie
6 Beveiliging
7 Accountantscontrole
8 Juridische zaken
9 Anders, nl:

2.20 Eigen vrachtwagens - Beschikt uw bedrijf over eigen en/of geleasde vrachtwagens voor extern gebruik en zo ja, om hoeveel vrachtwagens gaat het?

1 Weet niet/wil niet zeggen
2 Ja, _____ vrachtwagens voor extern gebruik
3 Nee, geen eigen vrachtwagens voor extern gebruik (Ga door naar vraag 2.22)

2.21 Aandeel extern transport - Kunt u aangeven welk deel van het externe transport door u is uitbesteed aan externe vrachtwagens/chauffeurs wordt verricht?

1 Weet niet/wil niet zeggen
2 Ja, _____ %

2.22 Certificering - Is uw bedrijf ISO 9001: 2000 (Kwaliteitsmanagement) en/of TAPA gecertificeerd?

1 Weet niet/wil niet zeggen
2 Ja, beide
3 Ja, ISO
4 Ja, TAPA
5 Nee, geen van beide

2.23 Omzet - Kunt u aangeven hoe groot de omzet van uw bedrijf was over 2003?

1 Weet niet/wil niet zeggen
2 Ja, € _____ miljoen

2.24 Verzekering - Kunt u aangeven of, en indien ja, op welke manier u bent verzekerd tegen schade, verlies en/of diefstel? Is dit…

1 Weet niet/wil niet zeggen
2 Nee, niet verzekerd, omdat ___
3 Ja, met totaalpakket voor o.a. gebouwen, inventaris en bedrijfsmiddelen
4 Ja, met een goederen totaalpakket
5 Ja, met logistiek totaalpakket (inclusief handelsgoederen)
6 Ja, met losse verzekeringen per bedrijfsobject
7 Ja, met losse verzekeringen per zending/evenement
8 Anders, nl:

2.25 Zaken onverzekerd - Zijn er zaken zoals bedrijfsmiddelen, handelsgoederen, financiële middelen en frauderisico's die bijv. vanwege de hoge premie of het hoge eigen risico niet zijn verzekerd tegen schade, verlies en/of diefstal? Zo ja, welke zijn dit en kunt u een toelichting geven?

1 Weet niet/wil niet zeggen
2 Nee, alles is verzekerd
3 Ja, de volgende zaken zijn niet verzekerd omdat:

2.26 Prestatie-indicatoren - Houdt uw bedrijf de kwaliteit van de leveringen bij m.b.v. prestatie-indicatoren zoals de ordercompleetheid? Zo ja, kunt u aangeven hoe hoog deze bij uw bedrijf ligt?

1 Weet niet/wil niet zeggen
2 Nee, dat houden wij niet bij omdat:
3 Ja, de ordercompleetheid ligt ongeveer op _____%
4 Ja, de _____ ligt op _____%

2.27 Resultaatverplichting - Werken uw bedrijf en/of uw opdrachtgevers met een resultaatverplichting, dat wil zeggen, zijn er marges waarbinnen schade, verlies en/of diefstal aanvaardbaar zijn?

1 Weet niet/wil niet zeggen
2 Nee, dergelijke marges tolereren wij en onze opdrachtgevers niet
3 Ja, vanuit opdrachtgevers geldt een marge van _____%
4 Ja, wij hanteren een marge van _____%

2.28 Opkoop beschadigde goederen - Kunnen werknemers beschadigde goederen tegen gereduceerde prijzen opkopen?

1 Weet niet/wil niet zeggen
2 Nee
3 Ja
4 Soms, onder voorwaarde dat ____
5 Soms, alleen bij de volgende producten ____

3 Risico's en preventiebeleid

Wij zijn in dit onderzoek geïnteresseerd in interne criminaliteit en interne normovertredingen*. Hiermee bedoelen we gedragingen van werknemers die strafbaar zijn volgens wettelijke bepalingen (criminaliteit)of gedragingen die ingaan tegen algemene sociale regels die ook in uw bedrijf gelden. Ook doelen wij hierbij steeds op incidenten die zich op elk niveau in de organisatie kunnen afspelen. In het vervolg zal ik gemakshalve alleen spreken over interne criminaliteit, maar weet dan dat ik ook niet-criminele normovertredingen bedoel.*
Het gaat ons om opzettelijke *gedragingen van werknemers die gericht zijn tegen uw bedrijf, dus waarbij uw* bedrijf het doelwit *vormt (en bijv. niet leveranciers of collega's). Met* werknemers *bedoelen we alle personen die ten behoeve van dit bedrijf of ter plaatse van dit bedrijf werkzaamheden verrichten, zoals personen die in dienst zijn van dit bedrijf, maar ook werknemers van ingehuurde bedrijven, van leveranciers, stagiaires, etc. Iedereen die vanuit de aard van zijn/haar werkzaamheden*

in staat is om dit bedrijf schade te berokkenen. Overigens kunnen hierbij ook buitenstaanders (externen) betrokken zijn, zolang er maar sprake is van 'interne betrokkenheid'. *We zijn vooral geïnteresseerd in incidenten die afzonderlijk, of door hun frequentie een* schade *opleveren die het bedrijf als problematisch ervaart. (Leg uit: we willen triviale normovertredingen uitsluiten, zoals het mee naar huis nemen van pennen, overmatig internetgebruik en privé-bellen,* check *of dit duidelijk is voor respondent).*

Ik ga u nu een paar vragen voorleggen over de risico's waar uw bedrijf op dit vlak mogelijk mee te maken heeft.

3.1 Risicovormen interne criminaliteit - Zijn er bepaalde vormen van interne criminaliteit die voor uw bedrijf een relatief groot schaderisico vormen? Zo ja, kunt u aangeven welke vormen van interne criminaliteit voor uw bedrijf het grootste schaderisico vormen?

1 Weet niet/wil niet zeggen
2 Nee, er zijn geen vormen van interne criminaliteit met bovengemiddeld risico
3 Ja, de belangrijkste vormen van interne criminaliteit zijn (geordend naar schaderisico):

3.2 Doelwitten interne criminaliteit - Wat zijn vanuit het oogpunt van schaderisico volgens u de belangrijkste doelwitten in uw bedrijf (overlap met vorige vraag mogelijk)?

1 Weet niet/wil niet zeggen
2 Nee, er zijn geen doelwitten met verhoogd risico
3 Ja, de belangrijkste doelwitten zijn:

3.3 Plaatsen interne criminaliteit - Zijn er bepaalde plekken binnen of buiten de muren van uw bedrijf (fysiek/geografisch) waar een verhoogd risico bestaat op interne criminaliteit (overlap met vorige vragen mogelijk)?

1 Weet niet/wil niet zeggen
2 Nee, er zijn geen plekken met verhoogd risico
3 Ja, de plekken met een verhoogd risico zijn:

3.4 Bedrijfsprocessen interne criminaliteit - Zijn er in uw bedrijf bepaalde bedrijfsprocessen of onderdelen van de bedrijfsvoering waarbij een verhoogd risico bestaat op interne criminaliteit (overlap met vorige vragen mogelijk)?

1 Weet niet/wil niet zeggen
2 Nee, er zijn geen specifieke processen/onderdelen met verhoogd risico
3 Ja, de bedrijfsprocessen en/of -onderdelen met een verhoogd risico zijn:

3.5 Periodes interne criminaliteit - Zijn er in uw bedrijf bepaalde periodes waarbij een verhoogd risico bestaat op interne criminaliteit (overlap met vorige vragen mogelijk)? (Int: Licht toe. Het kan gaan om periodes in een jaar, bepaalde dagen van de week, bepaalde tijdstippen op een dag).

1 Weet niet/wil niet zeggen
2 Nee, er zijn geen periodes etc. met verhoogd risico
3 Ja, periodes etc. met een verhoogd risico zijn:

3.6 Risico's vergelijkbare bedrijven - Denkt u dat vergelijkbare bedrijven die in dezelfde branche opereren ongeveer dezelfde schaderisico's t.a.v. interne criminaliteit ervaren als uw bedrijf? Zo nee, kunt u aangeven in welke opzichten volgens u andere bedrijven in de branche qua risicoprofiel afwijken van uw bedrijf?

1 Weet niet/wil niet zeggen
2 Ja, andere bedrijven hebben grosso modo dezelfde risico's omdat:
3 Nee, andere bedrijven hebben grosso modo meer/minder/ andere risico's omdat:

Ik wil nu met u kijken naar de maatregelen die uw bedrijf mogelijk neemt om te voorkómen dat interne criminaliteit zich kan voordoen. Ook wil ik het met u hebben over de mogelijkheden en beperkingen van preventieve maatregelen. (Int: preventieve maatregelen kunnen heel breed zijn. Voor ons zijn

ALLE maatregelen van belang die tenminste OOK gebruikt worden om interne criminaliteit tegen te gaan)

3.7 Preventieve maatregelen - Wilt u van de volgende preventieve maatregelen aangeven of uw bedrijf hiervan gebruik maakt. Een kort ja/nee antwoord volstaat.

1 Het bedrijfsterrein is door middel van hekwerken en poorten afgescheiden van de openbare weg
2 Er zijn obstakels geplaatst om ramkraken te voorkomen
3 Het bedrijfsterrein is vrijgehouden van opklimmogelijkheden (afvalcontainers, bomen, ladders)
4 Ramen en deuren zijn extra versterkt/vergrendeld
5 Het terrein en het gebouw zijn 's nachts extern verlicht
6 Er is een toegangscontrole om het terrein op of het gebouw binnen te komen
7 Er wordt gewerkt met toegangspasjes
8 Er zijn duidelijke afsluitprocedures
9 Het gebouw beschikt over een alarmsysteem dat in verbinding staat met een beveiligingsorganisatie of de politie
10 Er zijn buiten camera's opgehangen om het terrein in de gaten te houden
11 Er hangen binnen toezichtcamera's om personen en goederen in de gaten te houden
12 Er zijn signalen geplaatst dat het bedrijf goed beveiligd is
13 Waardevolle goederen en zaken worden extra beveiligd in kluizen en/of afgesloten bedrijfsruimten
14 Er is personele beveiliging op het bedrijfsterrein aanwezig
15 Richtlijnen omtrent de bestraffing en de gevolgen in geval van normovertredingen zijn voor werknemers duidelijk
16 Werknemers worden op de hoogte gehouden van gevallen van normovertredingen door andere werknemers
17 Er is een visitatieregeling voor het zonodig fouilleren van personeel
18 Voordat een nieuwe werknemer wordt aangenomen wordt zijn (criminele) voorgeschiedenis gescreend
19 Werknemers worden getraind om verdacht gedrag te herkennen en te rapporteren
20 Het computernetwerk is beveiligd tegen extern misbruik
21 Het computernetwerk is beveiligd met verschillende wachtwoorden op verschillende niveaus
22 Back-ups van computerbestanden worden minimaal wekelijks gemaakt
23 Fraudebeleid is een integraal onderdeel van het ondernemingsbeleid
24 Er zijn vastgelegde procedures om fraude te voorkomen
25 Procedures worden systematisch gecontroleerd
26 Het bedrijf werkt met een duidelijke functiescheiding

3.8 Overige maatregelen - Worden er in uw bedrijf nog belangrijke maatregelen genomen die wij hiervoor nog niet hebben besproken?

1 Weet niet/wil niet zeggen
2 Nee
3 Ja, nl:

3.9 Effectiviteit maatregelen - Wat is in het algemeen uw opinie over de effectiviteit van allerhande preventieve maatregelen die in uw branche gebruikelijk zijn? Welke maatregelen zijn volgens u bijzonder effectief en welke zijn bijzonder ineffectief? Kunt u een toelichting geven?

1 Weet niet/wil niet zeggen
2 Algemene opinie over maatregelen:
3 Bijzonder effectief volgens respondent:
4 Bijzonder ineffectief volgens respondent:

3.10 Obstakels maatregelen - Doen zich bij het realiseren van preventieve maatregelen in uw bedrijf beperkingen of obstakels voor? Zo ja, op welke vlakken liggen deze? (Denkt u hierbij bijvoorbeeld aan beperkingen of obstakels binnen of buiten het bedrijf, aan economische, financiële, organisatorische, juridische of andere beperkingen/obstakels om een gewenst veiligheidsniveau te bereiken)

1 Nee, geen beperkingen/obstakels bekend
2 Ja, ik zie de volgende obstakels:

3.11 Tevredenheid ondersteuning - Bent u tevreden over de ondersteuning die u vanuit de overheid en/of de brancheorganisaties krijgt om uw bedrijf beter te beveiligen? Zo nee, wat zouden deze kunnen doen om bedrijven te ondersteunen bij het nemen van preventiemaatregelen?

1 Weet niet/wil niet zeggen
2 Ja, tevreden over ondersteuning omdat:
3 Nee, niet tevreden, verbetering gewenst t.a.v.:

3.12 Monitoring - Ik leg u nu een aantal concrete activiteiten voor, die al of niet in uw bedrijf plaatsvinden. Wilt u per activiteit die ik noem aangeven of deze ook in uw bedrijf plaatsvindt? Een kort ja/nee antwoord volstaat.

1 Er wordt een overzicht bijgehouden van criminele incidenten of onregelmatigheden die zich hebben voorgedaan in het bedrijf
2 Er wordt een overzicht bijgehouden van zoekgeraakte handelsgoederen en bedrijfsmiddelen
3 Er wordt een overzicht bijgehouden van beschadigde handelsgoederen en bedrijfsmiddelen
4 Het bedrijf gebruikt een warehousemanagementsysteem
5 Er wordt gebruik gemaakt van een track & trace systeem voor goederen in het bedrijf\
6 Alle in- en uitgaande goederen in het bedrijf worden fysiek gecontroleerd
7 Voorraden worden regelmatig fysiek geïnventariseerd
8 Er wordt gebruik gemaakt van compartimentering van bedrijfsruimten, waarbij bepaalde werknemers een beperkte toegang hebben (niet iedereen kan overal in het bedrijf komen).
9 Er wordt gewerkt met een sleutel- en sluitplan waarin is vastgelegd welke personen op welke tijdstippen en plaatsen geautoriseerd en verantwoordelijk zijn voor het toegankelijk maken en afsluiten van ruimtes in het bedrijf
10 De aanwezigheid van niet-werknemers (zoals leveranciers, gasten, onderaannemers e.d.) die zich op enig moment in of rond het bedrijf ophouden wordt te allen tijde geregistreerd
11 Telefoon, email- en/of internetverkeer van werknemers wordt tenminste af en toe gescreend op onregelmatigheden
12 Het bedrijf is zo georganiseerd dat de werkzaamheden van bijna alle werknemers (ook die van leidinggevenden) op enige wijze gecontroleerd worden door andere werknemers of de directie
13 De financiële bedrijfsvoering wordt jaarlijks door een extern accountant gecontroleerd
14 Door werknemers ingediende kostendeclaraties worden steekproefsgewijs of structureel gecontroleerd op onregelmatigheden
15 Het bedrijf heeft gewenst en ongewenst gedrag van werknemers vastgelegd in een schriftelijke gedragscode
16 Lijnfunctionarissen in de organisatie zijn in de meeste gevallen getraind in het onderkennen van risicosignalen bij hun medewerkers
17 Het bedrijf stimuleert door middel van concrete activiteiten dat werknemers elkaar aanspreken op kleine normovertredingen
18 Het bedrijf schakelt incidenteel of vaker externe beveiligingsexperts in om een risico-analyse te maken

3.13 Functionering bedrijfscode (Alleen als het bedrijf gebruikt maakt van een bedrijfscode) - Hoe functioneert de bedrijfscode binnen uw bedrijf?

1 Weet niet/wil niet zeggen
2 Goed, want:

3 Redelijk, want:
4 Niet goed, want:
5 Anders, nl:

3.14 Reden afwezigheid bedrijfscode (Alleen als het bedrijf geen gebruik maakt van een bedrijfscode) - Heeft uw bedrijf wel eens nagedacht over het opstellen van een bedrijfscode? Waarom wel of niet?

1 Weet niet/wil niet zeggen
2 Nee niet over bedrijfscode nagedacht, want:
3 Ja, wel over nagedacht, maar:
4 Anders, nl:

4 Aard en omvang van gesignaleerde criminaliteit (extern en intern)

Ik ga nu een aantal vragen stellen over criminaliteit in het algemeen en interne criminaliteit in het bijzonder waar uw bedrijf mogelijk mee te maken heeft gehad.

4.1 Externe criminaliteit een probleem - Beschouwt u criminaliteit door buitenstaanders als een probleem voor uw bedrijf? (noem 5 categorieën)

1 Weet niet/wil niet zeggen
2 Heel groot probleem
3 Groot probleem
4 Enigszins/soms een probleem
5 Nauwelijks een probleem
6 In het geheel geen probleem
7 Anders, nl:

4.2 Interne criminaliteit een probleem - Beschouwt u interne criminaliteit en andere normovertredingen door werknemers als een probleem voor uw bedrijf? (noem 5 categorieën)

1 Weet niet/wil niet zeggen
2 Heel groot probleem
3 Groot probleem
4 Enigszins/soms een probleem
5 Nauwelijks een probleem
6 In het geheel geen probleem
7 Anders, nl:

Ik wil u nu graag een aantal vragen voorleggen over concrete vormen van criminaliteit en andere normovertredingen waar uw bedrijf in de afgelopen 3 jaar mogelijk mee geconfronteerd is. Het kan hierbij gaan om zowel interne als externe criminaliteit. Als uw bedrijf slachtoffer is geworden van één of meer van de zaken die ik ga noemen, zal ik u daar enkele korte vervolgvragen over stellen, zoals het aantal incidenten dat zich heeft voorgedaan, of er mogelijk interne mensen bij betrokken waren, wat de schade is geweest en dergelijke. We zijn alleen geïnteresseerd in normovertredingen die, afzonderlijk of in zijn totaliteit, een schadepost hebben opgeleverd die het bedrijf als problematisch ervaart en sluiten triviale normoverredingen en niet-geslaagde pogingen dus uit (Int: spreek over deel van organisatie waar respondent kijk op heeft – zie blok 3! Deel dit nogmaals mede aan respondent).

4.3 Is uw bedrijf (*of het deel waar resp. zicht op heeft*) in de afgelopen 3 jaar wel eens slachtoffer geworden van de volgende normovertredingen? (Int: aankruisen Ja/Nee/Weet niet. *Als Ja, dan uitwerken in losse schema's*).

1 Overval met geweld - Hebben personen uw bedrijf schade berokkend door een bedrijfsgebouw, -terrein, een transportmiddel of enig ander doelwit te *overvallen*, waarbij

handelsgoederen, bedrijfsmiddelen of andersoortige zaken zijn buitgemaakt? (criterium: geweldgebruik of dreiging met geweld tegen personen)

2 Inbraak - Hebben personen uw bedrijf schade berokkend door *in te breken* in een afgesloten bedrijfsgebouw, bedrijfsterrein, transportmiddel of enig ander doelwit (bijv. computernetwerk), waarbij handelsgoederen, bedrijfsmiddelen of andersoortige zaken (bijv. informatie) zijn buitgemaakt?

3 Vervalsing - Hebben personen uw bedrijf schade berokkend door het vervalsen of *niet naar waarheid opmaken van schriftelijke documenten* of andersoortige administratieve opgaven (bijv. sjoemelen met vrachtbrieven of kostendeclaraties)?

4 Oplichting - Hebben personen uw bedrijf schade berokkend door *oplichting*, d.w.z. dat ze onder *valse voorwendsels* uw bedrijf hebben bewogen tot het beschikbaar stellen van geld, goederen, gegevens, rechten e.d. (bijv. door zich als iemand anders of ander bedrijf voor te doen)?

5 Onterechte rechtentoekenning - Hebben personen uw bedrijf schade berokkend door op niet toegestane wijze zichzelf bepaalde *rechten toe te kennen* (waarna bijv. allerlei onkosten gedeclareerd kunnen worden)?

6 Doorspelen bedrijfsgegevens - Hebben personen uw bedrijf schade berokkend door vertrouwelijke en/of waardevolle *bedrijfsgegevens door te spelen* aan derden en/of deze gegevens openbaar te maken (bijv. verkopen gegevens aan concurrent)? (zonder koppeling aan andere normovertredingen zoals inbraak e.d.)

7 Aanbestedingen - Hebben personen uw bedrijf schade berokkend door werknemers van uw bedrijf privé-voordelen te bieden bij het gunnen van *diensten of aanbestedingen* waardoor aanbestedingen duurder dan nodig uitvielen?

8 Eenvoudige diefstal - Hebben personen uw bedrijf schade berokkend door zichzelf *geld* of goederen van uw bedrijf toe te eigenen waartoe zij door de uitoefening van hun werk toegang hadden? Bijvoorbeeld diefstal geld remboursementen (criterium: niet door inbraak, overval, fraude, oplichting e.d. verkregen). Let op: maak eventueel onderscheid tussen geld, goederen en voertuigen.

9 Opzettelijke beschadiging - Hebben personen uw bedrijf schade berokkend door met opzet gebouwen, bedrijfsmiddelen, handelsgoederen of andersoortige zaken die uw bedrijf bezit of beheert te *beschadigen of te vernietigen*? (bijv. d.m.v. brandstichting, infecteren van computersystemen, etc.)

10 Handel illegale goederen - Hebben personen uw bedrijf schade berokkend door *middelen* die uw bedrijf toebehoren te gebruiken *voor de handel in illegale goederen of diensten* (zoals bijv. handel in drugs, kinderporno, e.d.)?

11 Bedrijfsmiddelen voor commercie - Hebben personen uw bedrijf schade berokkend door *middelen* die uw bedrijf toebehoren te gebruiken *voor commerciële activiteiten* ten eigen bate (bijv. in het weekend met vrachtwagen van bedrijf als verhuizer bijverdienen)? (criterium: géén handel in illegale goederen of diensten)

12 Bedrijfsmiddelen voor privé - Hebben personen uw bedrijf schade berokkend door *middelen* die uw bedrijf toebehoren te gebruiken *voor privé-doeleinden*? (criterium: niet commercieel)

13 Sabotage - Hebben personen uw bedrijf schade berokkend door opzettelijk reguliere *bedrijfsprocessen te saboteren* (bijv. door afspraken opzettelijk verkeerd te plannen of ongeoorloofd niet aanwezig te zijn)? (criterium: geen beschadiging van bedrijfsmiddelen etc.)

14 Verwijtbare nalatigheid - Hebben personen uw bedrijf schade berokkend door *verwijtbare nalatigheid* of onoplettendheid (oftewel schade door verwijtbaar onprofessioneel handelen)? (criterium: géén opzet)

15 *Bullying* of geweld - Hebben personen uw bedrijf schade berokkend door opzettelijk werknemers te bedreigen, niet toe te laten of weg te pesten?

Zijn er nog andere vormen van criminaliteit of normovertredingen die ik niet genoemd heb, maar waar dit bedrijf in de afgelopen 3 jaar wel slachtoffer van is geworden (en schade van heeft ondervonden)?

a Nee (Ga door naar vraag 4.4)

b Ja, nl:

4.4 Vergelijking eerdere jaren - We hebben nu een overzicht samengesteld van concrete incidenten die zich in de afgelopen tijd hebben voorgedaan in dit bedrijf. Wijkt dit overzicht in belangrijke mate af van de situatie in voorgaande jaren (bijv. meer, minder of andere incidenten, minder schade, minder zicht op daders, minder aangifte)? Zo ja, op welke wijze (Int: open vraag, noteer bijzonderheden)?

1 Weet niet/wil niet zeggen
2 Nee, geen verschillen
3 Ja, anders want meer/minder/andere _____ omdat:

4.5 Vergelijking andere bedrijven - Hebt u het idee dat bedrijven die op uw bedrijf lijken en die in dezelfde branche opereren in dezelfde mate met dezelfde problemen te maken hebben als die u hiervoor genoemd heeft? Zo ja, licht toe. Zo nee, welke verschillen ziet u tussen dit bedrijf en andere bedrijven in de branche (Int: open vraag, noteer bijzonderheden)?

1 Weet niet/wil niet zeggen
2 Ja, bedrijven hebben dezelfde problemen omdat
3 Nee, vergelijkbare bedrijven hebben meer/minder/andere problemen, nl:

4.6 *Dark number* - Het is soms moeilijk om erachter te komen wat er in een bedrijf zoal speelt als het gaat om interne criminaliteit. Immers, niet alle incidenten laten zichtbare sporen na en als dit wel het geval is, is niet altijd duidelijk of er opzet in het spel is en of er in dat geval ook interne mensen bij betrokken waren. Men spreekt in dit verband wel over het *dark number*: dit zijn incidenten waar het bedrijf om allerlei redenen geen zicht op heeft of kan krijgen. Herkent u dit probleem?

1 Weet niet/wil niet zeggen
2 Nee, eventueel toelichting (Ga door naar vraag 5):
3 Ja, toelichting:

4.7 Vormen criminaliteit en schade - Kunt u aangeven welke vormen van criminaliteit u hier denkt aan te treffen en hoe groot de schade van dit dit *dark number* ongeveer is?

1 Weet niet/wil niet zeggen
2 Ja, nl:

4.8 Maatregelen - Zijn er bijzondere maatregelen die uw bedrijf neemt om deze moeilijk zichtbare vormen van interne criminaliteit beter in beeld te krijgen?

1 Weet niet/wil niet zeggen
2 Nee
3 Ja, nl:

4.9 Daderkenmerken - Zijn er, naar uw ervaring, bepaalde kenmerken aan te wijzen waaraan plegers van interne criminaliteit of interne normovertredingen herkend kunnen worden? Het gaat ons om kenmerken die opvallend vaak vóórkomen en die betrekking hebben op de persoon van de pleger, zijn/haar achtergrond, zijn/haar relatie tot dit bedrijf, de werkomstandigheden, etc.

1 Weet niet/wil niet zeggen
2 Nee, er zijn geen standaard daderkenmerken aan te wijzen
3 Ja, daders hebben naar mijn idee de volgende kenmerken:
    a Demografische kenmerken pleger, nl:
    b Persoonlijkheidskenmerken pleger, nl:
    c Criminele antecedenten of vroeger probleemgedrag van pleger, nl:
    d (Sociale) privé-situatie pleger, nl:
    e Kenmerken van dienstverband (soort/duur), nl:
    f Kenmerken van functie, nl:
    g Kenmerken van werkomstandigheden waarin pleger functioneert, nl:
    h Werkhouding van pleger, nl:
    i Opvattingen van pleger over (aspecten) van bedrijf(-svoering), nl:
    j Overige kenmerken van pleger, nl

Aantal observaties - Kunt u ongeveer aangeven op hoeveel waarnemingen deze observaties gebaseerd zijn? (deze waarnemingen mogen ook betrekking hebben op gevallen die zich elders, d.w.z. buiten uw bedrijf en/of tijdens eerdere werkervaring, hebben voorgedaan)

1 Weet niet/wil niet zeggen
2 Dit is gebaseerd op _____ gevallen, toelichting:

5 Vervolg van incidenten in het strafrechtsysteem

Tot slot wil ik u enkele vragen voorleggen over het doen van aangifte bij de politie en de eventuele gang naar het strafrecht

5.1 Aantal keren aangifte - In hoeveel gevallen van normovertredingen waarbij mogelijk sprake was van interne betrokkenheid heeft u de afgelopen drie jaar aangifte gedaan bij de politie?

1 Weet niet/wil niet zeggen
2 Niet van toepassing, want geen gevallen
3 Nooit
4 Zelden, maar wel in _____ gevallen
5 Regelmatig, in _____ gevallen
6 Altijd, in _____ gevallen

5.2 Algemeen beleid aangifte - Kunt u aangeven wat in het algemeen het beleid van uw bedrijf is ten aanzien van het doen van aangifte bij de politie en welke motivatie ligt hieraan ten grondslag?

1 Weet niet/wil niet zeggen
2 Wij doen nooit aangifte, omdat (Ga door naar vraag 5.11):
3 Wij hebben geen concreet beleid. Soms wordt aangifte gedaan, soms niet. De criteria verschillen per geval. Toelichting:
4 Wij doen altijd aangifte, want
5 Wij doen alleen aangifte (meerdere antwoorden mogelijk)
   a Ten behoeve van de verzekering, want
   b Ten behoeve van opdrachtgevers, want
   c Bij een minimaal schadebedrag, want
   d Als de (vermoedelijke) dader(s) bekend is (zijn), want
   e In het geval dat

5.3 Actie politie - Wat deed de politie de afgelopen twee jaar met uw aangifte en in welke gevallen volgde een opsporingsactie (meerdere antwoorden mogelijk)?

1 Weet niet/wil niet zeggen
2 Nooit opsporingsactie
3 Altijd opsporingsactie, in alle _____ gevallen
4 Zaak loopt nog in _____ gevallen
5 Alleen opsporingsactie in die _____ gevallen dat er concrete verdachten/zeker schadebedrag/geweld gebruikt was/waren:

5.4 Kennisgeving actie politie - Hoe raakt u op de hoogte van wat er met uw aangiften gebeurt?

1 Weet niet/wil niet zeggen
2 De politie stelt mij altijd op de hoogte
3 De politie stelt mij nooit op de hoogte
4 De politie stelt mij op de hoogte als niks/opsporingsactiviteiten/uitkomst onderzoek:
5 De politie stelt mij alleen op de hoogte na informatieverzoeken van mijn kant
6 De politie stelt mij zelfs niet op de hoogte na informatieverzoeken

5.5 Vervolging OM - In hoeveel gevallen waarbij u de afgelopen twee jaar aangifte heeft gedaan, heeft dit geleid tot vervolging door het Openbaar Ministerie (meerdere antwoorden mogelijk)?

1 Weet niet/wil niet zeggen

2 Nooit vervolging (Ga door naar vraag 5.10)
3 Altijd vervolging, in alle _____ gevallen dat aangifte werd gedaan
4 Zaak loopt nog in _____ gevallen
5 Alleen vervolging in die _____ gevallen dat er concrete verdachten/zeker schadebedrag/geweld gebruikt was/waren:

5.6 Kennisgeving vervolging - Hoe raakt u op de hoogte van eventuele vervolging?
1 Weet niet/wil niet zeggen
2 Via de werknemer
3 Via de politie
4 Via de politie na informatieverzoek
5 Het OM stelt mij altijd op de hoogte
6 Het OM stelt mij nooit op de hoogte
7 Het OM stelt mij alleen op de hoogte als niks/vervolging:
8 Het OM stelt mij alleen op de hoogte na informatieverzoeken van mijn kant
9 Het OM stelt mij zelfs niet op de hoogte na informatieverzoeken

5.7 Veroordeling justitie - In hoeveel gevallen waarbij tot vervolging is overgegaan, heeft dit geleid tot veroordeling door justitie (meerdere antwoorden mogelijk)?
1 Weet niet/wil niet zeggen
2 Nooit veroordeling (Ga door naar vraag 5.10)
3 Altijd veroordeling, in alle _____ gevallen dat tot vervolging werd overgegaan
4 Zaak loopt nog in _____ gevallen dat tot vervolging werd overgegaan
5 Alleen veroordeling in die _____ gevallen dat er concrete verdachten/zeker schadebedrag/geweld gebruikt was/waren:

5.8 Veroordeling tot - In die gevallen waarin tot veroordeling werd overgegaan, waartoe werd(en) verdachte(n) veroordeeld?
1 Weet niet/wil niet zeggen
2 Geldboete in _____ gevallen
3 Leer of werkstraf in _____ gevallen
4 Vrijheidsstraf in _____ gevallen
5 Combinatiestraf in _____ gevallen
6 Anders, in _____ gevallen, nl:

5.9 Kennisgeving veroordeling - Hoe raakt u op de hoogte van eventuele veroordeling?
1 Weet niet/wil niet zeggen
2 Via de werknemer
3 Via de politie
4 Via de politie na informatieverzoek
5 Via het OM
6 Via het OM na informatieverzoek
7 Justitie stelt mij nooit op de hoogte
8 Justitie stelt mij altijd op de hoogte
9 Justitie stelt mij op de hoogte als niks/veroordeling:
10 Justitie stelt mij alleen op de hoogte na informatieverzoeken van mijn kant
11 Justitie stelt mij zelfs niet op de hoogte na informatieverzoeken

5.10 Proces-verbaal beschikbaar stellen - Wij overwegen om de aangiften die bedrijven zoals het uwe in de laatste drie jaar hebben gedaan bij de politie, in kaart te brengen om in alle gevallen vast te stellen welke vervolgactiviteiten er precies hebben plaatsgevonden bij politie en justitie en tot welke uitkomsten dit heeft geleid. Zou u hieraan mee willen werken door het beschikbaar stellen van de betreffende proces-verbaal nummers? Uiteraard gaan wij hier strikt vertrouwelijk mee om.
1 Nee, respondent wil niet meewerken

2 Ja, respondent wil meewerken (afspraak omtrent verkrijgen proces-verbaal nummers)

5.11 Tevredenheid strafrechtapparaat - Bent u tevreden over wat het strafrechtapparaat (politie, justitie, rechterlijke macht) voor uw bedrijf betekent bij het voorkómen en aanpakken van interne criminaliteit? Zo nee, wat zou er kunnen verbeteren?

1 Weet niet/wil niet zeggen
2 Bedrijf maakt nauwelijks of geen gebruik van strafrecht, handelt zaken intern af.

Toelichting:

3 Ja, tevreden omdat:
4 Nee, niet tevreden, verbetering gewenst ten aanzien van:

6 Overige opmerkingen respondent

Hiermee zijn we aan het einde gekomen van dit interview. Ik wil u hier echter nog de ruimte geven voor eventuele slotopmerkingen die u mij als onderzoeker, het ministerie van justitie als opdrachtgever of de belangenorganisaties als belangenbehartiger nog mee zou willen geven.

6.1 Slotopmerkingen - Zijn er nog zaken die u kwijt wilt of die u nog extra wil benadrukken?

1 Nee
2 Ja, nl:

Dan wil ik u nu graag hartelijk danken voor de tijd die u voor mij heeft vrij gemaakt. U houdt natuurlijk het eindrapport en de reader van ons te goed.

7 Observaties interviewer

7.1 Observaties - (Int: ruimte voor eigen observaties) Wat viel mij op? Hoe was de houding van de respondent? Hoe liep het gesprek?

Bijlage 2 Vragenlijst deel 2: Uitwerking normovertredingen

1 Nummer - Nummer normovertreding (1-15):

_____

2 Aantal incidenten - Hoeveel incidenten waren er in de afgelopen 3 jaar?
- a Weet niet/wil niet zeggen
- b _____

3 Interne betrokkenheid - In hoeveel van deze gevallen was sprake was van concrete of vermoedelijke betrokkenheid van interne mensen?
- a Weet niet/wil niet zeggen
- b Geen (Ga door met de volgende normovertreding)
- c _____

4 Schade - Wat was de totale schade van de incident(en) waarbij werknemers betrokken waren?
- a Weet niet/wil niet zeggen
- b € _____

5 Identiteit werknemer bekend - Van hoeveel incidenten waarbij vermoedelijk werknemers betrokken waren is de identiteit van de werknemer bekend geworden?
- a Weet niet/wil niet zeggen
- b _____

6 Vervalt

Uitwerking laatste soortgelijke normovertreding waarbij sprake was van interne betrokkenheid (Int: eventueel langer dan 12 maanden geleden)

7 Tijdstip - Wanneer en in welke periode vond de laatste normovertreding plaats?

8 Beschrijving incident - Kunt u een beschrijving geven van het soort delict/incident (Int: een zaak kan uit meerdere gebeurtenissen bestaan)?

9 Doelwit/buit - Wat was het doelwit/de buit?

10 Aan het licht - Hoe kwam(en) incident(en) aan het licht?
- a Weet niet/wil niet zeggen
- b Heterdaad
- c Melding werknemer
- d Melding pleger
- e Anonieme melding
- f Direct zichtbare delictsporen (bijv. braak/geweld/alarm/detectie)
- g Bij de uitvoering van reguliere bedrijfsactiviteiten (bijv. ontbreken spullen)
- h Bij de uitvoering van (reguliere of speciale) controlemaatregelen
- i Door een melding van de opdrachtgever
- j Anders, nl:

11 Acties intern en extern - Welke actie(s) heeft het bedrijf intern en extern genomen na het aan het licht komen van het incident (meerdere antwoorden mogelijk)
- a Weet niet/wil niet zeggen
- b Geen actie

Interne actie
- a Intern onderzoek instellen, nl:
- b Aanpassen beveiliging, nl:
- c Aanpassen bedrijfsprocessen, nl:
- d Anders, nl:

Externe actie
- a Melden bij politie (geen aangifte)
- b Aangifte politie
- c Inschakelen particulier recherchebureau
- d Inschakelen veiligheids- of risicoadviseur
- e Inschakelen (forensisch) accountant
- f Inschakelen overige deskundigen
- g Inlichten omringende bedrijven/belanghebbenden/brancheorganisaties
- h Anders, nl:

12 Dader bekend geworden - Is de dader van het incident bekend (geworden)?
- a Nee (Besluit uitwerking van deze normovertreding met vraag 13)
- b Ja (Ga verder met vraag 14 tot en met 18)

13 Standaardprocedure - Is de manier waarop u met dit incident bent omgegaan te bestempelen als standaardprocedure? Zo nee, welke maatregelen neemt het bedrijf normaal gesproken bij dergelijke incidenten met onbekende dader(s)?
- a Weet niet/wil niet zeggen
- b Geen actie
- c Ja, reactie was standaardprocedure (Ga door naar volgende normovertreding)
- d Nee, reactie was anders, nl (Ga door naar volgende normovertreding):

14 Bekendwording identiteit dader - Hoe kwam de identiteit van de dader(s) aan het licht?
- a Weet niet/wil niet zeggen
- b Heterdaad
- c Melding werknemer
- d Melding pleger
- e Anonieme melding
- f Intern onderzoek, nl:
- g Extern onderzoek, nl:
- h Anders, nl:

15 Kenmerken dader - Wat zijn de kenmerken van deze dader(s) en kunt u dit toelichten?
- a Weet niet/wil niet zeggen
- b Demografische kenmerken pleger, nl:
- c Persoonlijkheidskenmerken pleger, nl:
- d Criminele antecedenten of vroeger probleemgedrag van pleger, nl:
- e (Sociale) privé-situatie pleger, nl:
- f Kenmerken van dienstverband (soort/duur), nl:
- g Kenmerken van functie, nl:
- h Kenmerken van werkomstandigheden waarin pleger functioneert, nl:
- i Werkhouding van pleger, nl:
- j Opvattingen van pleger over (aspecten) van bedrijf(-svoering), nl:
- k Overige kenmerken van pleger, nl:

16 Acties tegen dader - Welke acties zijn ondernomen tegen de dader(s)
- a Weet niet/wil niet zeggen
- b Geen maatregelen getroffen
- c Mondelinge berisping/waarschuwing
- d Schriftelijke berisping/waarschuwing
- e Aantekening in personeelsdossier
- f Onbetaald schorsen
- g Ontnemen van bepaalde rechten/toegang
- h Demotie (negatieve promotie)
- i Herplaatsing in bedrijf (naar andere plek/functie)

j Openbaar maken van identiteit van werknemer in bedrijf
k Vrijwillig ontslag (na aandringen bedrijf)
l Gedwongen ontslag
m Aangifte bij politie
n Teruggeven van goederen/compensatie van schade (onderlinge regeling)
o Betalen van (geld)boete (onderlinge regeling)
p Verhalen van schade via civiele rechter
q Verhalen van schade via strafrechter
r Anders, nl:

17 Standaardprocedure - Is de manier waarop u met dit incident bent omgegaan te bestempelen als standaardprocedure? Indien niet, welke maatregelen neemt het bedrijf dan normaal gesproken bij dergelijke normovertredingen met bekende dader(s)?

a Weet niet/wil niet zeggen
b Geen actie
c Ja, reactie was standaardprocedure (Ga door naar volgende normovertreding)
d Nee, reactie was anders, nl:

18 Civiele procedure - (Alleen in geval van civiele procedure) Kunt u mij zeggen wat de afloop was van deze civiele procedure?

a Weet niet/wil niet zeggen
b Zaak is nog in behandeling
c Schadevergoeding toegewezen, nl:
d Schadevergoeding afgewezen, omdat

Bijlage 3 Overzicht van geïnterviewde experts

Vertrouwelijk

Bijlage 4 Overzicht van de leden van de begeleidingscommissie 'Interne Criminaliteit in de Logistieke Sector'

Voorzitter

Prof. dr. G.A.A.J. van den Heuvel
Bijzonder hoogleraar Criminologie
Universiteit van Maastricht (voorzitter)

Namens opdrachtgever

Dr. F.W. Beijaard
Projectbegeleider
Ministerie van Justitie (WODC/EWB), Den Haag (namens opdrachtgever)

Overige leden

Prof. dr. H. Elffers
Senior onderzoeker/ hoogleraar Rechtspsychologie
Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Leiden / Universiteit Antwerpen

Drs. F.M.M. de Kort
Beleidsmedewerker
Ministerie van Justitie (DGPJS/DSP), Den Haag

Mevr. H. Minderman
Juridisch beleidsmedewerker
Transport en Logistiek Nederland, Zoetermeer

Dr. mr. H.J.B. Sackers
Universitair hoofddocent Strafrecht
Radboud Universiteit Nijmegen

Mr. drs. R.G.J. Wildemors
Beleidsmedewerker
Ministerie van Justitie (DGPJS/DSP), Den Haag

Bijlage 5 Afkortingenlijst

ACN	Air Cargo Netherlands
AIVD	Algemene Inlichtingen en Veiligheidsdienst
BRT	Boven Regionaal Team
CBP	College Bescherming Persoonsgegevens
CBS	Centraal Bureau voor de Statistiek
CJD	Centrale Justitiële Documentatie
CMR	Convention relative au contrat de transport internationale de Marchandises par Route
FIOD-ECD	Fiscale Inlichtingen- en Opsporingsdienst/Economische Controledienst
ISPS	International Ship and Port Facility Security
JDS	Justitieel Documentatiesysteem
KLPD	Korps Landelijke Politiediensten
KMar	Koninklijke Marechaussee
KNV	Koninklijk Nederlands Vervoer
KvK	Kamer van Koophandel
LDV	Logistiek Dienstverlener
LTT	Landelijk Team Transportcriminaliteit
NDL	Nederland Distributieland
NPC	Nationaal Platform Criminaliteitsbeheersing
OvJ	Officier van Justitie
OM	Openbaar Ministerie
PDG	Physical Distribution Group
PV	Proces-verbaal
RM	Rechterlijke macht
TAPA	Technology Asset Protection Association
TLN	Transport en Logistiek Nederland
VAL	Value Added Logistics
VAS	Value Added Services
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum