Veiligheidsbarometer voor ondernemingen: een explorerende studie naar de beveiliging in ondernemingen en slachtofferschap

Studienr. 1

Auteurs: Dormaels Arne & Verwee Isabel

Verantwoordelijke Uitgever: Karin Genoe

Uitgever: Vias institute – Security and Innovation

Dit onderzoek werd mogelijk gemaakt dankzij de samenwerking met het VBO, UNIZO, Unisoc, Agrofront, UCM, UWE.

Inhoudstafel

Lijst van figuren en tabellen

1. Executive summary

Vias institute lanceerde de Veiligheidsbarometer: een verkennend onderzoek dat nagaat hoe veiligheid en beveiliging op de agenda worden gezet in ondernemingen en hoe zij zich wapenen in de strijd tegen criminaliteit. De bevraging werd uitgevoerd in de periode van juli tot en met oktober 2018, bij 273 Nederlands- en Franstalige ondernemingen uit verschillende sectoren.

Goed voorbereid?

Opvallend: in bijna de helft van de bevraagde ondernemingen worden weinig of geen controles georganiseerd op vlak van beveiliging. 43,4% zei dat er geen beleid uitgetekend is om de onderneming te beveiligen tegen criminaliteit, 19,87% gaf aan dat er geen beveiligingsmaatregelen genomen worden en 37,66% van de bevraagde personen had niet het gevoel dat zijn of haar bedrijf voldoende voorbereid is op eventuele veiligheidsincidenten.

67,07% van de ondernemingen gaf aan in één of meerdere systemen geïnvesteerd te hebben om zich fysiek of organisatorisch te beveiligen. De meest voorkomende investeringen zijn sloten, camerabewaking en alarmsystemen. In 28,99% van de bedrijven voert men ook een doorgedreven screening uit bij de aanwerving van nieuwe medewerkers.

Cybercriminaliteit als risico

Wanneer respondenten gevraagd werden de risico's waaraan hun onderneming blootgesteld wordt in te schatten, kwamen vooral verschillende vormen van cybercriminaliteit als grote risico's naar voren. Maar liefst een derde van de ondernemingen achtte het '(helemaal) wel waarschijnlijk' dat ze in het komende jaar slachtoffer zullen worden van bijvoorbeeld hacking of phishing. Ook 'tussenkomst in data of systemen door middel van virussen, cryptoware of DDoS-aanvallen' (27,23%) en internetfraude (20,56%) haalden de top vijf.

Ook bedrijven die het niet per se waarschijnlijk achtten dat ze het komende jaar slachtoffer zullen worden, hechtten belang aan IT-beveiliging. Maar liefst 93,84% van de respondenten gaf aan dit belangrijk te vinden. De meeste ondernemingen hanteren een aantal basisregels. Zo maakt 96,48% regelmatig back-ups van gegevens, houdt 92,96% de besturingssystemen steeds up-to-date en beveiligt 92,96% de wifitoegang. 72,6% heeft een specifiek beveiligingsbeleid op IT-niveau.

Toch is er heel wat ruimte voor verbetering. Zo gaf 23,94% van de ondernemingen aan geen wachtwoordenbeleid te hebben. In 44,52% van de ondernemingen zorgt men bovendien niet regelmatig voor opleidingen of training rond IT-beveiliging of actuele bedreigingen en 24,65% sensibiliseert haar personeel niet rond veelvoorkomende IT-dreigingen.

Imago is alles?

Wanneer ondernemingen investeren in veiligheid, doen ze dat hoofdzakelijk om personen (bv. medewerkers en/of klanten) te beschermen. 38,46% van de bedrijven gaf dit aan als hoofdreden. Andere redenen zijn het beschermen van de infrastructuur (18,27%), de informatie (15,39%) en de producten of diensten van het bedrijf (13,46%). Slechts 1,92% van de ondernemingen gaf de bescherming van het imago op als hoofdreden.

78,08% van de respondenten vond dat veiligheid in de onderneming de verantwoordelijkheid is van de werkgever. 67,81% stelde dat ook elke individuele werknemer in de onderneming een verantwoordelijkheid draagt.

Criminele feiten op de werkvloer: geen ver-van-mijn-bed-show

Aan ondernemingen die zeiden géén veiligheidsmaatregelen te nemen, werd gevraagd waarom. Bijna de helft (48,84%) gaf aan 'dat het risico om slachtoffer te worden te klein is'. Nochtans toont deze barometer aan dat de kans om als onderneming slachtoffer te worden van criminele feiten wel reëel is. Maar liefst 42,6% van de deelnemende ondernemingen werd in de 12 maanden voorafgaand aan de studie slachtoffer van één of meerdere vormen van cybercriminaliteit. Een hoog cijfer, wetende dat er wellicht nog veel meer ondernemingen zijn waarop cybercriminelen het gemunt hadden. Daarnaast waren ook beschadiging van een voertuig (41,91%), geweld en agressie (39,71%), beschadiging van eigendommen of vandalisme (39,71%) en ongeoorloofde toegang zonder geweld (38,24%) veelvoorkomende feiten.

Aangeven of zelf oplossen?

In het laatste onderdeel van de barometer werd, bij ondernemingen die in het afgelopen jaar slachtoffer werden van minstens één crimineel feit, gepeild naar het 'meest ingrijpende' feit. De slachtoffers duidden 'geweld en agressie' (19,3%), 'cybercriminaliteit: illegale toegang tot IT-systemen' (8,77%) en 'ongeoorloofde toegang zonder geweld' (7,9%) aan als meest ingrijpend. Opvallend: meer dan een kwart van de ondernemingen (28,32%) deed géén aangifte van dit feit bij de politie. 'Omdat dit toch geen resultaat oplevert' en 'omdat men er toch niks aan kan doen,' aldus respectievelijk 28,13% en 12,5% van deze bedrijven. 15,63% deed geen aangifte 'omdat we de dader kennen' en nog eens 12,5% 'omdat we de zaak niet ernstig genoeg vonden'.

Opnieuw meer dan een kwart (28,83%) van de ondernemingen die slachtoffer werden, gaf aan dat ze het criminele feit zelf probeerde op te lossen, bijvoorbeeld door de dader zelf te zoeken en/of aan te spreken, de schade in der minne te regelen, … In de meerderheid van de gevallen kostte deze oplossing het bedrijf minder dan een dag werktijd en minder dan 5.000 euro.

Werknemerscriminaliteit

De veiligheidsbarometer toont aan dat ondernemingen die slachtoffer werden van een crimineel feit de dader ervan in 28,32% van de gevallen kenden. In meer dan een derde van die gevallen ging het om een werknemer van de onderneming zelf of een contractor.

Interne meldpunten en vertrouwenspersonen

In 36,80% van de ondernemingen bestond er op het moment van het onderzoek geen procedure voor het melden van verdachte handelingen op of naast de werkvloer. In 45,60% van de bedrijven was er geen anoniem meldpunt voorzien. Vooral in kleinere ondernemingen werd dit vaak niet formeel vastgelegd. De vraag is dus of werknemers van deze organisaties voldoende weten waar ze terecht kunnen als ze slachtoffer of getuige zijn van een crimineel feit op de werkvloer.

Ook in de nasleep van een crimineel feit is het niet altijd duidelijk waar werknemers met hun vragen of zorgen terecht kunnen. 24,80% van de deelnemende ondernemingen gaf aan dat er geen vertrouwenspersoon aanwezig is waarbij werknemers terecht kunnen om over hun ervaringen te praten. 15,20% zei dat er geen psychosociale opvangmogelijkheden zijn (intern of extern) voor werknemers die met criminaliteit te maken kregen.

2. Context

Meer dan ooit is veiligheid een relevant en actueel thema in onze samenleving, alsook in de ondernemingswereld. Vias institute lanceert een barometer die nagaat hoe veiligheid en beveiliging op de agenda worden gezet bij ondernemingen en hoe men zich wapent in de strijd tegen criminaliteit. Het vergaren van inzicht door middel van deze barometer is cruciaal om een realistisch beeld te krijgen over hoe ondernemingen bezig zijn met veiligheid en zich beschermen tegen mogelijk slachtofferschap van criminaliteit. Om die informatie te krijgen, deden wij beroep op de medewerking van organisaties die de ondernemingssector vertegenwoordigen.

Dit onderzoek kadert binnen het streven naar een veiligheidscultuur in alle geledingen van de Belgische samenleving. Zowel overheid, ondernemingen en organisaties als burgers worden bewustgemaakt van de opportuniteiten en bedreigingen die de huidige maatschappelijke context met zich meebrengt. Het nastreven van een weerbare samenleving, waarin ondernemingen, organisaties en burgers zich weerbaar opstellen tegen potentiële risico's en bedreigingen, staat hierin cruciaal.

De veiligheidsbarometer voor ondernemingen werd geconstrueerd in samenspraak met de verschillende partners en bevat verschillende modules. Het betreft een barometer waarbij gekeken werd in welke mate ondernemingen en KMO's bezig zijn met veiligheid en zich wapenen in de strijd tegen criminaliteit. Deze bevraging gaat dus niet in op voedsel-, arbeids- en brandveiligheid maar op veiligheid gelinkt aan criminaliteit. De barometer gaat in op verschillende thema's zoals algemene aandacht voor beveiliging, risico-inschatting, veiligheidscultuur- en beleid, IT- en fysieke beveiliging en slachtofferschap.

De vragenlijst werd geprogrammeerd in key survey, waarbij met zoveel mogelijk voorgeprogrammeerde antwoordcategorieën werd gewerkt. Dit vereenvoudigde de analyse van de resultaten. De partners werden betrokken in de test en konden op basis van deze test hun opmerkingen doorgeven. Er werd zo veel mogelijk aan deze opmerkingen tegemoet gekomen, om vervolgens de veiligheidsbarometer te lanceren in de zomer van 2018.

In de periode van juli tot en met oktober 2018 werden ondernemingen uitgenodigd om deel te nemen aan de veiligheidsbarometer. Nadat de antwoorden op anonieme en globale wijze waren verwerkt, werd er met de partnerorganisaties gereflecteerd over de resultaten in een interactieve werksessie (IW). In deze interactieve sessie was het enerzijds de bedoeling om in te gaan op wat de cijfers betekenen voor de ondernemingswereld. Anderzijds maakte de sessie het ook mogelijk om te bespreken hoe er verder aan de slag kon worden gegaan met de resultaten. Hierdoor werden inzichten in cijfers gegenereerd en werden de resultaten van de bevraagden gecontextualiseerd.

In dit rapport zullen de resultaten die voortvloeien uit de bevraging worden beschreven. Daarnaast zullen ook een aantal bedenkingen, reflecties en contextualiseringen van de deelnemers aan de IW (de hieronder opgesomde partners) worden besproken. Tot slot worden aanbevelingen geformuleerd.

Dit onderzoek kwam tot stand dankzij de medewerking van verschillende partners/organisaties die ondernemingen vertegenwoordigen. We wensen de volgende partners uitdrukkelijk te bedanken: de federaties van het Verbond voor Belgische Ondernemingen, Unizo, Unisoc, Agrofront, Union des classes moyennes (UCM) en Union Wallonne des Entreprises (UWE).

3. Onderzoeksresultaten

3.1 Respons rate en achtergrondkenmerken van de ondernemingen

Aan deze barometer namen 273 respondenten deel, waarvan 79,5% de vragenlijst in het Nederlands invulde en 20,5% in het Frans.

89,97% van de respondenten gaf aan dat het zwaartepunt van de activiteiten van zijn of haar onderneming zich situeert op het nationale niveau. 10,04% gaf dus aan dat het zwaartepunt van hun economische activiteiten in het buitenland ligt. De provincies in België die het vaakst werden aangeduid betreffen Oost-Vlaanderen, Antwerpen, het Brussels Hoofdstedelijk Gewest en West-Vlaanderen.

Er zijn heel wat kleine tot middelgrote ondernemingen die deze bevraging invulden. Op de vraag 'Hoeveel medewerkers werken er in uw onderneming?', treffen we de volgende percentages aan:

- 34,43% tussen 0 – 10 medewerkers
- 17,22% tussen 11 – 50 medewerkers
- 19,41% tussen 51 - 250 medewerkers
- 10,26% tussen 251 – 500 medewerkers
- 7,33% tussen 501 – 1000 medewerkers
- 11,36% meer dan 1001 medewerkers

Op de vraag of de bevraagde een leidinggevende functie heeft, gaf 77,29% aan dat dit het geval is. 22,71% had dus geen leidinggevende functie.

De sector waarin de onderneming zich in hoofdzaak situeert, was:

- 16,35% vervoer en opslag
- 15,97% menselijke gezondheidszorg en maatschappelijke dienstverlening
- 13,69% landbouw, bosbouw en visserij
- 11,03% bouwnijverheid
- 8,75% 'andere'
- 7,99% voedingsindustrie
- 6,46% financiële activiteiten en verzekeringen
- 6,84% industriesector
- …

3.2 Werknemers besteden minder aandacht aan beveiliging in een onderneming dan werkgevers

	Helemaal niet akkoord					Helemaal wel akkoord	Weet niet/geen antwoord
Onze onderneming besteedt aandacht aan beveiliging	2,90%	1,45%	5,31%	9,18%	24,16%	54,59%	2,42%
Onze directie besteedt aandacht aan beveiliging	2,90%	2,42%	5,31%	10,15%	22,22%	55,07%	1,93%
Onze medewerkers besteden aandacht aan beveiliging	3,38%	5,80%	6,76%	20,77%	30,92%	29,47%	2,90%
Er worden bewustmakingsactiviteiten in onze onderneming georganiseerd in het kader van beveiliging	8,21%	12,08%	9,18%	13,53%	22,71%	29,47%	4,83%
Er wordt regelmatig een test of een controle op het vlak van beveiliging georganiseerd in onze onderneming	18,84%	16,91%	11,59%	15,46%	14,49%	18,36%	4,35%

Tabel 1: Algemene aandacht voor veiligheid in een onderneming (N=207)

De respondenten werden gevraagd om op een schaal van 1 (helemaal niet akkoord) tot 6 (helemaal wel akkoord) aan te duiden in hoeverre zij akkoord gaan met bovenstaande stellingen. Een eerste resultaat dat in het oog springt, is dat 55,07% van de respondenten 'helemaal wel akkoord' ging met de stelling 'Onze directie besteedt aandacht aan beveiliging' en een gelijkaardig percentage (namelijk 54,59%) beaamde de stelling 'Onze onderneming besteedt aandacht aan beveiliging'. Dit in tegenstelling tot de stelling 'Onze medewerkers besteden aandacht aan beveiliging', waarbij slechts 29,47% 'helemaal wel akkoord' antwoordde. Dit cijfer is opvallend lager in vergelijking met 'onze onderneming' en 'onze directie'.

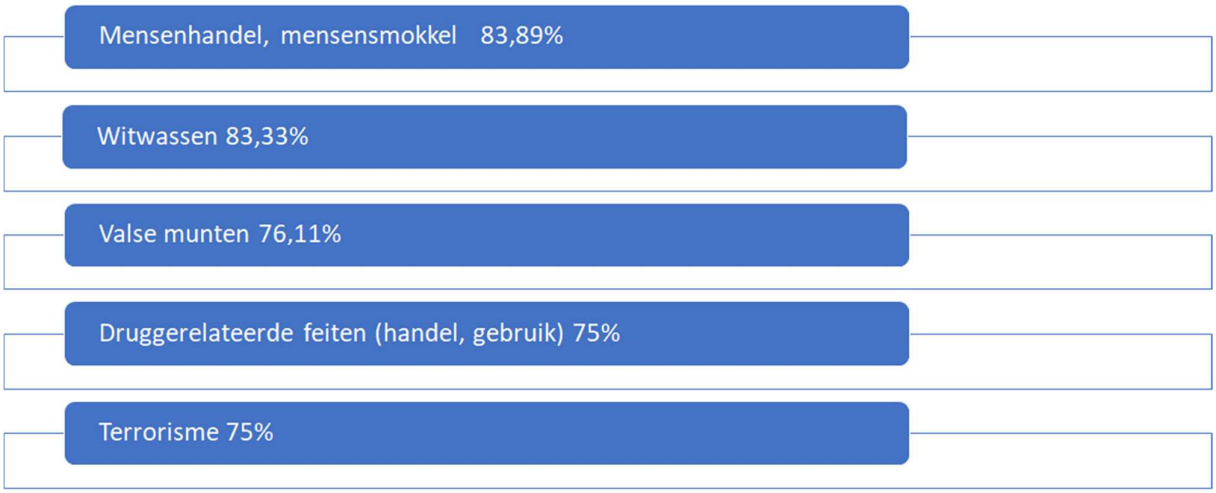
Een tweede opvallende bevinding was dat de respondenten het vaakst 'helemaal niet akkoord' of 'eerder niet akkoord' antwoordden bij de volgende stellingen: 'Er wordt regelmatig een test of een controle op het vlak van beveiliging georganiseerd in onze onderneming' en 'Er worden bewustmakingsactiviteiten in onze onderneming georganiseerd in het kader van beveiliging'.

De werkgever wordt het meest verantwoordelijk geacht voor de beveiliging van de onderneming en staat in voor de maatregelen om de veiligheid van het bedrijf te garanderen. Wat vaak wordt vergeten, is dat de werknemer een even belangrijke rol speelt in de beveiliging van de onderneming, zoals bijvoorbeeld door zorgvuldig om te gaan met paswoorden en updates te installeren. Zo stelt de federale overheid dat heel wat incidenten zouden kunnen vermeden worden indien de werknemers bewust worden van het belang van cybersecurity (Federale Overheidsdienst, 2017).

3.3 Cybercriminaliteit als risico

De vragenlijst bevatte een aantal specifieke vragen rond veiligheid. Zo werd de vraag gesteld in welke mate de onderneming in de volgende 12 maanden slachtoffer zou kunnen worden van vermelde vormen van criminaliteit. Er werden een aantal feiten als zeer waarschijnlijk aangeduid en andere feiten als minder waarschijnlijk.

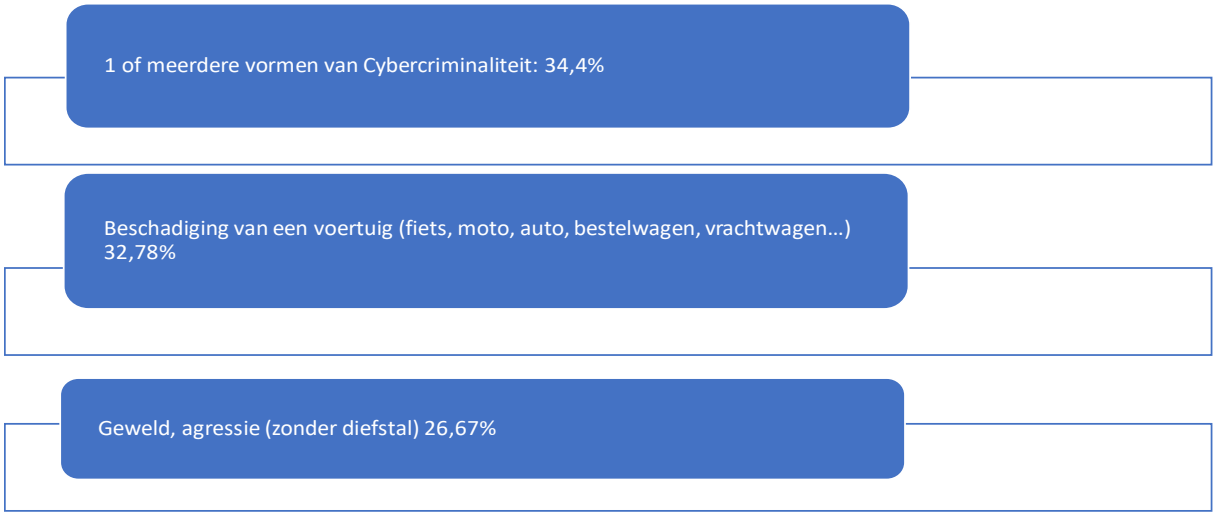
Dit is de top 5 van feiten waarvan men inschatte dat het 'helemaal niet waarschijnlijk' of 'niet waarschijnlijk' is dat men ervan slachtoffer zal worden.



Figuur 1: 'Helemaal niet waarschijnlijk', 'niet waarschijnlijk' slachtofferschap de komende 12 maanden (N = 180)

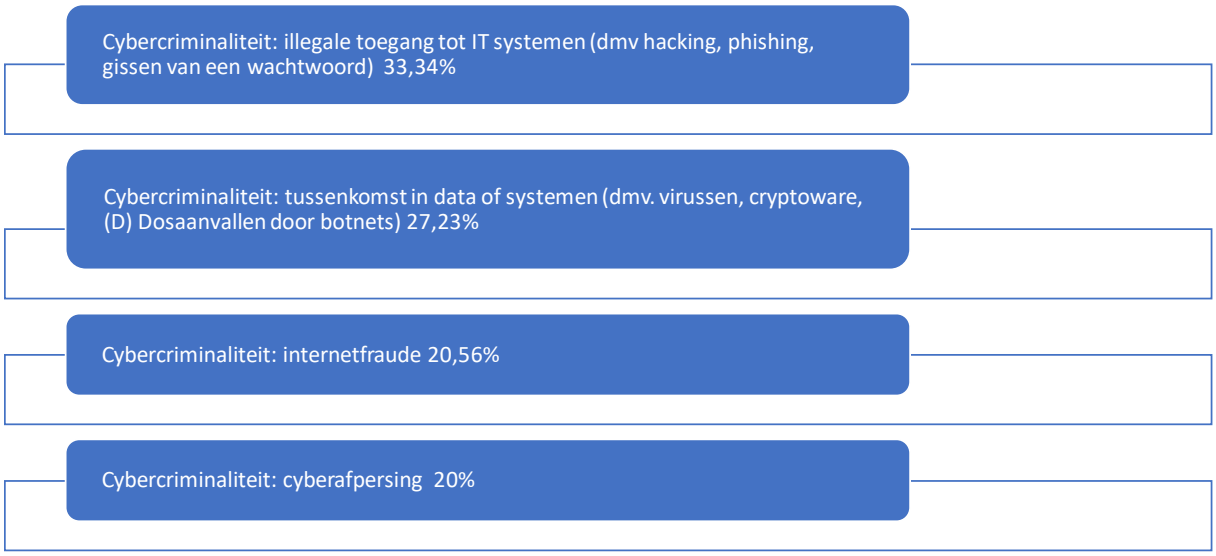
Uit figuur 1 blijkt dat de feiten 'mensenhandel, mensensmokkel' en 'witwassen' als minst risicovol werden gepercipieerd door de bevraagde ondernemingen. Eén van de mogelijke verklaringen wordt gezocht in de prevalentie van deze criminaliteitsvormen. Zo merken we dat het aantal aangiftes van mensenhandel de laatste jaren is afgenomen (Federale Politie, 2018; AD, 2019). Of dit het gevolg is van een werkelijke daling van de criminaliteit of eerder een daling betreft van het aantal meldingen is niet duidelijk, maar het kan wel zorgen voor een verminderde aandacht voor deze fenomenen, wat een verklaring kan zijn voor de verlaagde risico-inschatting. Dit verband gaat evenwel niet op voor druggerelateerde feiten en terrorisme. Er is volgens Belga een expansie van de productie van cannabis en synthetische drugs in België (Belga, 2018) en volgens het Europees Parlement een toename van terroristische dreigingen en aanslagen van jihadistische aard (Europees Parlement, 2018).

Het criminele feit dat als het grootste risico werd beschouwd (gaande van 'waarschijnlijk' tot 'helemaal wel waarschijnlijk') betreft cybercriminaliteit. 34,4% van de ondernemingen duidde een vorm van cybercriminaliteit aan als een 'helemaal wel waarschijnlijk' of 'waarschijnlijk' risico om er de komende 12 maanden slachtoffer van te worden.



Figuur 2: 'Helemaal wel waarschijnlijk, 'waarschijnlijk' slachtofferschap de komende 12 maanden (N=180)

In de navolgende tabel ziet u per vorm van cybercriminaliteit hoe het slachtofferschap werd ingeschat.



Figuur 3: 'Helemaal wel waarschijnlijk, 'waarschijnlijk' slachtofferschap van een vorm van cybercriminaliteit de komende 12 maanden (N=180)

Op basis van figuur 2 zien we dat cybercriminaliteit als reëel risico wordt ingeschat: meer dan één derde van de respondenten gaf aan dit als een risico te ervaren. Omdat er heel wat vormen zijn van cybercriminaliteit, werd deze diversiteit voorgelegd aan de respondent. Cybercriminaliteit door middel van illegale toegangen tot systemen werd als grootste risico gepercipieerd. Het tweede grootste cyberrisico betrof tussenkomst in data of systemen door middel van virussen, cryptoware of (D)Dosaanvallen door botnets. Zo'n 20% van de bevraagden gaf aan dat zij zowel internetfraude als cyberafpersing als reëel risico ervaren voor de komende 12 maanden.

Deze inschatting kwam ook aan bod in het Global Risk Report. De groei van cybercriminaliteit uit zich zowel in de prevalentie als in haar disruptief potentieel: "*Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace*". Zo waren de grootste kosten in 2017 te wijten aan ransomware aanvallen, waarvan 64% kwaadaardige e-mails betroffen. Een andere groeiende trend is het gebruik van cyberattacks ten aanzien van kritische infrastructuren en strategische industriële sectoren die een bepaalde angst zaaien waarbij – in the worst case scenario – de zogenaamde 'attackers' een breakdown veroorzaken in datgene wat de samenleving draaiende houdt (World Economic Forum, 2018).

In de Global Risk Perception Survey (2018) gaf slechts 7% van de bevraagden aan dat er een daling is van het aantal risico's. Er zijn vier grote bezorgdheden: 1) persistente ongelijkheid en onfairheid, 2) huishoudelijke en internationale politieke spanningen, 3) omgevingsveranderingen en 4) cyberkwetsbaarheden.

In tegenstelling tot 2017, waarin men zich nog maar weinig zorgen maakte over de cyberrisico's, kwamen in 2018 cyberattacks en massale datafraude in de top 5 terecht van fenomenen waar men met een zekere graad van waarschijnlijkheid slachtoffer kan van worden.

Cyberinbreuken die werden geregistreerd door ondernemingen verdubbelden bijna op 5 jaar tijd: van 68 per onderneming in 2012 tot 130 per onderneming in 2017 (World Economic Forum, 2018). Cybercriminelen hebben een exponentieel stijgend aantal potentiële targets omdat het gebruik van clouddiensten accelereert en van *the Internet of Things* wordt verwacht dat het fors zal uitbreiden de komende jaren. Wat men vroeger als cyberattacks op kleine schaal beschouwde worden nu normale attacks. De attackers worden ook meer persistent en de financiële kost stijgt. Zo wordt er verwezen naar de financiële kost van de WannaCry attack. Naast de financiële kost tast dit ook kritische en strategische infrastructuren aan: "*the WannaCry attack disrupted critical and strategic infrastructure across the world, including government, ministries, railways, banks, telecommunications providers, energy companies, car manufacturers and hospitals*" (Global Risk Perception Survey, 2018).

Meerdere aanvallen op kritische en strategische systemen slaagden niet in hun opzet maar de combinatie van de geïsoleerde successen en een groeiende lijst van aanvalspogingen tonen aan dat de risico's ook groeiende

zijn. De groeiende interconnectiviteit in de wereld zorgt ervoor dat pogingen – als ze slagen – radicale en onomkeerbaar systematische schokken veroorzaken.

Aons' Global Risk Management Survey van 2017 werd ontwikkeld om organisaties een inzicht te geven in "*to compete in this increasingly complex operation environment*". Er werden 1843 beslissers van publieke en private bedrijven bevraagd uit kleine, medium en grote bedrijven in 33 industriesectoren en verspreid over 60 landen.

De resultaten tonen aan dat bedrijven te maken krijgen met heel wat nieuwe risico's, en dat er een gebrek is aan consensus over hoe we deze risico's prioriteren en erop reageren. Ook hier merken we op dat cyberrisico's in de top 5 van risico's staan, terwijl politieke risico's/onzekerheden de top 10 bereikten. De link tussen politieke risico's, onzekerheden en cybercriminaliteit wordt ook benadrukt door heel wat gebeurtenissen uit 2016, zoals een verhoging van de georganiseerde cybercriminaliteit, wat een directe impact had op gouvernementele instituties, politieke partijen en globale infrastructuren.

Er wordt een verschil in risico-inschatting opgemerkt naargelang de grootte van de bedrijven. Grotere bedrijven zullen veel sneller cyber crime/hacking/viruses/malicious code aanduiden als risico's in vergelijking met kleinere bedrijven (Aons' Global Risk Management Survey, 2017).

Een gelijkaardige risico-inschatting vinden we tot slot terug in de Allianz Risk Barometer van 2018 (opgemaakt aan de hand van inzichten van 1911 experten in het risicodomein uit 80 verschillende landen) waarin werd gewezen op business interruption als eerste toekomstige zorg en cybersecurity-incidenten als tweede belangrijkste zorg in de toekomst (Allianz Risk Barometer, 2018).

Naast cybercriminaliteit werden ook twee andere vormen van criminaliteit aangehaald in deze veiligheidsbarometer, namelijk de beschadiging van een voertuig (auto, moto, fiets) en geweld en agressie (zonder diefstal). Ook van deze feiten werd ingeschat dat de onderneming of een medewerker van de onderneming hier de komende 12 maanden slachtoffer kan van worden.

Als in ons onderzoek de risico-inschatting werd gekruist met de vraag 'Hoeveel medewerkers werken er in uw onderneming?' vonden we enkele statistisch significante verbanden[1]. We vonden een redelijk of matig verband bij geweld, agressie (zonder diefstal) en terrorisme. De respondenten die werken in kleinere bedrijven (meer bepaald bedrijven met minder dan 250 medewerkers) achtten het vaker 'helemaal niet waarschijnlijk', 'niet waarschijnlijk' of 'eerder niet waarschijnlijk' dat zij slachtoffer kunnen worden van geweld en agressie (zonder diefstal). Bij het fenomeen 'terrorisme' zagen we tevens dat de kleinere ondernemers frequenter 'helemaal niet waarschijnlijk' en 'niet waarschijnlijk' aanduidden, terwijl de grotere bedrijven iets genuanceerder antwoordden met 'niet waarschijnlijk' en 'eerder niet waarschijnlijk'.

3.4 Veiligheidscultuur, het management en het beleid inzake beveiliging in uw onderneming

3.4.1 Veiligheidsbeleid kennen en implementeren

Een derde thematiek die aan bod kwam in de barometer was de veiligheidscultuur, het management en het beleid inzake beveiliging in ondernemingen. 73,91% van de respondenten gaf aan een zicht te hebben op de wettelijke voorschriften en bepalingen inzake beveiliging in zijn of haar onderneming. 26,09% is hier niet van op de hoogte.

Op de vraag of men zicht heeft op de wijzigingen van wettelijke voorschriften en bepalingen inzake beveiliging in ondernemingen, antwoordde 68,94% 'ja' en 31,06% 'nee'. Daarnaast stelde 56,6% van de bevraagden dat

[1] Het kruisen van de variabelen laat toe om na te gaan of er een verband bestaat tussen beide. We kijken of het verband statistisch significant is en indien dit het geval is wordt de grootte van de associatiemaat bekeken. Binnen sociologisch/criminologisch onderzoek worden globaal genomen volgende richtlijnen gebruikt voor het uitdrukken van de sterkte van een verband:

- Zeer zwak/geen verband: 0 - .10
- Zwak verband: .11- .30
- Redelijk of matig verband: .31 - .50
- Sterk verband: .51 - .80
- Zeer sterk verband: .81 - .99
- Perfect verband: 1

er in de onderneming een beleid is om zich te beveiligen tegen criminaliteit en 43,4% gaf aan dat dit niet het geval is.

Om te kijken of er een statistisch significant verband is tussen de aanwezigheid van een beleid om zich te beveiligen tegen criminaliteit en het aantal werknemers in de organisatie, werden deze twee stellingen gekruist. Dit resulteerde in een redelijk of matig significant verband. Meerdere respondenten die werken in een kleine onderneming antwoordden 'nee' op de vraag of er in hun onderneming een beleid is om zich te beveiligen tegen criminaliteit. Deze bevinding wordt bevestigd door Techzine (2018). Zo wordt gesteld dat kleine en middelgrote bedrijven vaak een achterstand hebben op vlak van veiligheid. Zij werken vaak met beperktere budgetten en een beknopte technologische kennis (Techzine, 2018).

De personen die positief antwoordden op de vraag of er een beleid is om zich te beveiligen tegen criminaliteit kregen een vervolgvraag gesteld, met name of het beveiligingsbeleid werd aangepast binnen een tijdspanne van 24 maanden. De meerderheid van deze respondenten duidde aan van wel.

Een ruime meerderheid (namelijk 78,65%) gaf ook aan dat dit veiligheidsbeleid naar de medewerkers van de onderneming toe gecommuniceerd wordt, slechts 14,61% stelde dat dit niet gebeurt. 6,74% duidde 'weet niet/geen antwoord' aan.

Figuur 4: Neemt uw onderneming beveiligingsmaatregelen in de strijd tegen criminaliteit? (N=156)

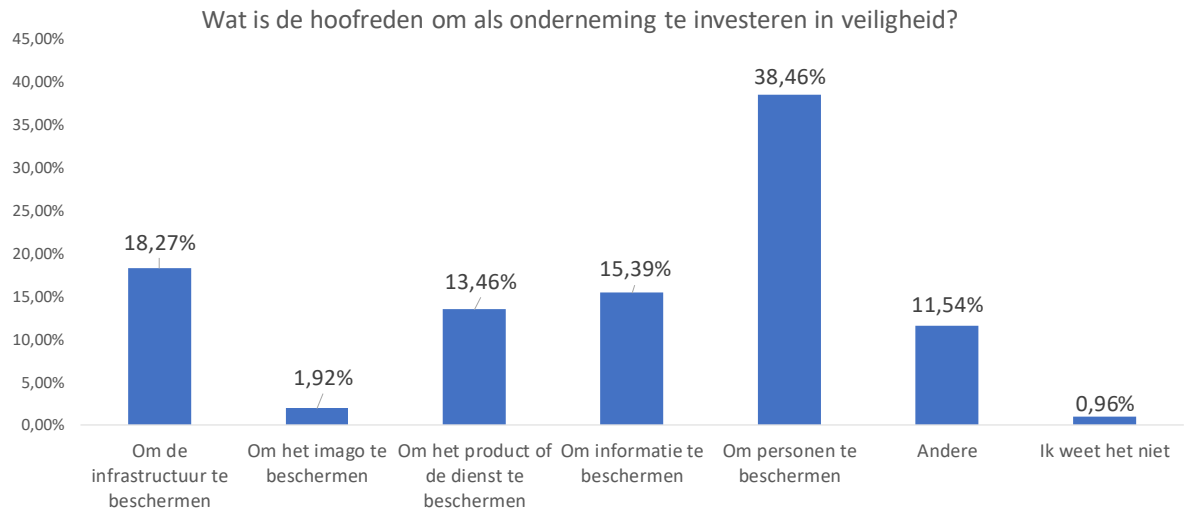
In bovenstaande figuur zien we dat 67,3% van de respondenten positief antwoordde op de vraag of zijn of haar onderneming beveiligingsmaatregelen neemt in de strijd tegen criminaliteit. 19,87% antwoordde 'nee', dus één vijfde van de ondernemingen gaf aan dat er geen maatregelen worden getroffen. Er is een groeiend bewustzijn binnen bedrijven omtrent de veiligheid, maar ondanks het groeiende bewustzijn worden er te weinig maatregelen getroffen (Belga, 2015). 12,82% duidde 'weet niet' aan of gaf geen antwoord.

Van de ondernemingen die 'ja' antwoordden, vond 75% dit gepaste of juiste maatregelen, 5,77% vond dit niet en 19,23% duidde 'weet niet/geen antwoord' aan.

UNIZO bevroeg 783 leden naar hun beveiligingsbeleid. Er werd onder meer gepolst waarom men weinig tot niets investeerde in een veiligheidsbeleid. Ongeveer 30% van de bevraagden gaf aan dat zij niet op de hoogte zijn van de mogelijkheden die ze kunnen nemen om zich te beschermen. Een vierde stelt dat de kosten niet opwegen tegen de baten. Tot slot stelt 40% dat het risico om slachtoffer te worden te beperkt is (UNIZO, 2016).

3.4.2 Investeren in veiligheid = beschermen van personen, infrastructuur en informatie

De door de respondenten aangegeven hoofredenen om als onderneming te investeren in veiligheid worden in onderstaande figuur weergegeven.



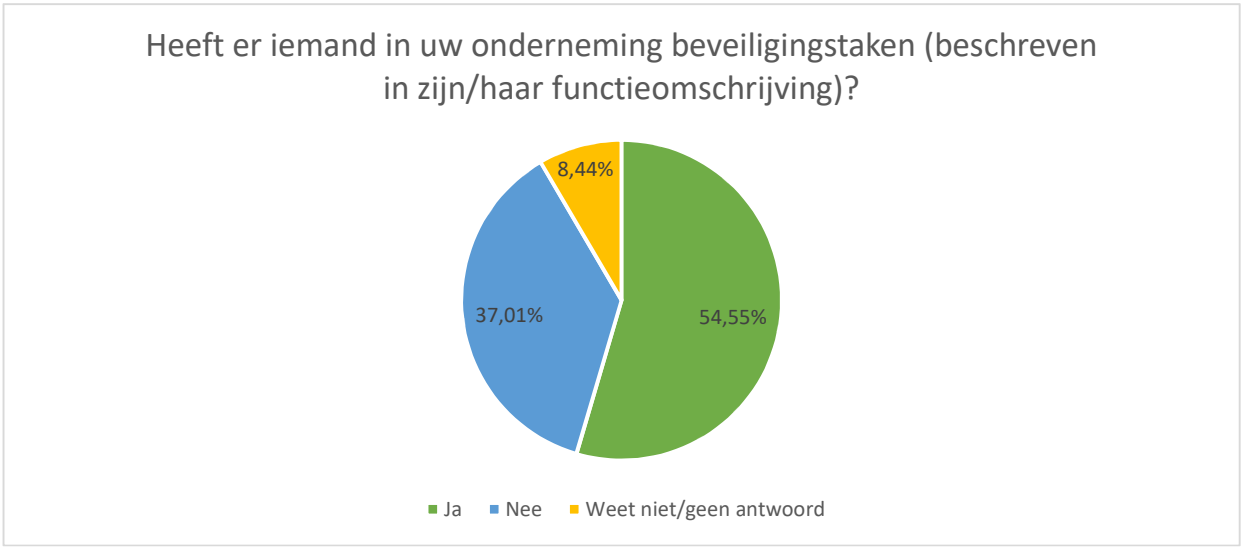
Figuur 5: Wat is de hoofdreden om als onderneming te investeren in veiligheid? (N=104)

De hoofdredenen om als onderneming te investeren in veiligheid zijn:

1. het beschermen van personen
2. het beschermen van de infrastructuur
3. het beschermen van de informatie
4. het beschermen van het product of de dienst

Op de vraag of het mogelijk is om de veiligheidsmaatregelen in het bedrijf aan te passen in functie van mogelijke dreigingen, bijvoorbeeld na een verhoging van het OCAD-dreigingsniveau, antwoordde 61,54% positief. Eén vijfde van de respondenten (namelijk 20,19%) gaf geen antwoord of wist dit niet. 18,27% antwoordde 'nee'.

Aan de respondenten die aangaven dat hun onderneming geen veiligheidsmaatregelen neemt, werd gevraagd waarom. Bijna de helft van deze respondenten – namelijk 48,84% - gaf aan dat 'het risico om slachtoffer te worden klein is'. 18,61% antwoordde dat men niet op de hoogte is van wat de mogelijkheden zijn om zich te beveiligen. 13,95% stelde dat de kosten te hoog zijn, terwijl 11,63% vond dat er een tijdsgebrek is.



Figuur 6: Heeft er iemand in uw onderneming beveiligingstaken? (N=154)

Zoals in bovenstaande figuur wordt weergegeven, werd ook gevraagd of bepaalde personen in de onderneming beveiligingstaken hebben. De meerderheid van de bevraagden gaf aan dat er in de onderneming

medewerkers zijn voor wie beveiligingstaken omschreven staan in de functieomschrijving. 37,01% stelde dat dit niet het geval is en 8,44% wist dit niet of gaf geen antwoord.

Als we deze vraag kruisten met het aantal medewerkers in een onderneming, vonden we een significant verband: erg kleine ondernemingen (0-10 medewerkers) duidden het vaakst 'nee' of 'weet niet/geen antwoord' aan.

De vraag 'Doet u beroep op een externe firma in het kader van de beveiliging, bijvoorbeeld om u te beveiligen tegen bepaalde criminaliteitsproblemen?' werd door iets meer dan de helft van de bevraagden negatief beantwoord. 52,94% antwoordde 'nee', terwijl 43,79% 'ja' antwoordde. Het overige percentage wist het niet of gaf geen antwoord. Op de vraag of men op de hoogte is van de maatregelen die deze externe firma neemt, gaf 86,57% aan op de hoogte te zijn van de genomen maatregelen. 71,64% overlegt regelmatig met deze externe firma en 14,93% overlegt niet regelmatig met de externe firma.

3.4.3 Niet elke onderneming is in staat om veiligheidsrisico's te detecteren

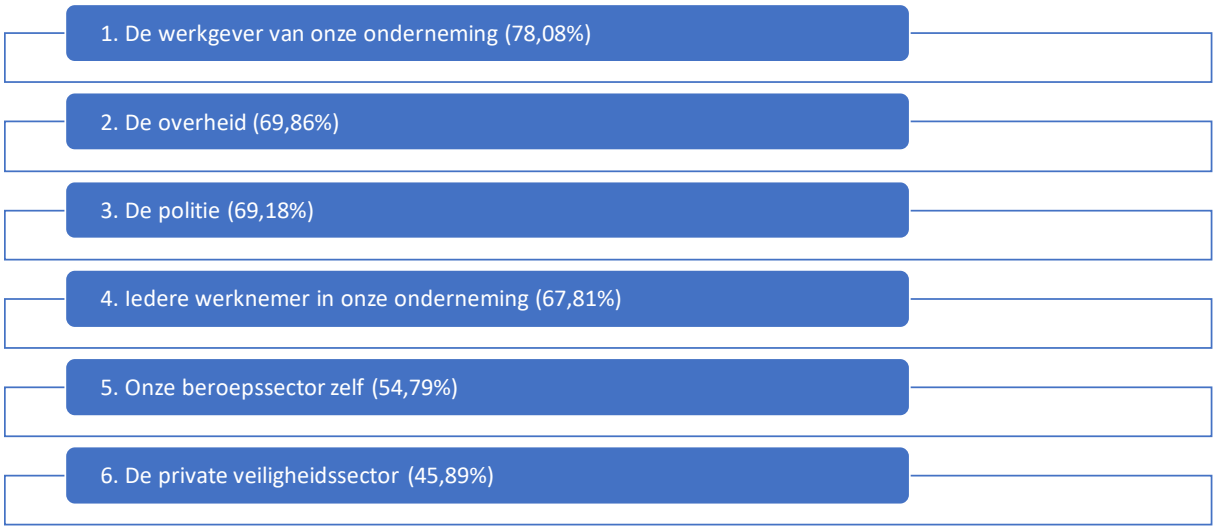
	Helemaal niet akkoord	Niet akkoord	Eerder niet akkoord	Eerder wel akkoord	Wel akkoord	Helemaal wel akkoord	Weet niet/geen antwoord
Onze onderneming is in staat om veiligheidsrisico's te detecteren	6,85%	9,59%	17,12%	14,38%	25,34%	22,60%	4,11%
Onze onderneming is voorbereid voor als er zich beveiligingsincidenten voordoen	8,90%	15,75%	13,01%	15,07%	27,40%	15,75%	4,11%
Er is een plan van aanpak aanwezig voor als er zich een beveiligingsincident voordoet	11,64%	15,75%	10,27%	17,12%	26,03%	14,38%	4,80%

Tabel 2: Kan u aangeven in hoeverre u akkoord gaat met... (N=146)

Op de stelling 'Onze onderneming is in staat om veiligheidsrisico's te detecteren' antwoordde 62,32% 'helemaal wel akkoord' tot 'eerder wel akkoord'. Dit betekent dat ongeveer 33% van de respondenten vindt dat de onderneming niet of eerder niet in staat is om veiligheidsrisico's te detecteren. Iets minder dan 60% (namelijk 58,22%) ging 'helemaal akkoord' tot 'eerder wel akkoord' met de stelling dat de onderneming voorbereid is op mogelijke veiligheidsincidenten. 37,66% ging 'helemaal niet akkoord' tot 'eerder niet akkoord' met deze stelling. Dezelfde percentages vonden we terug bij de stelling 'Er is een plan van aanpak aanwezig voor als er zich een beveiligingsincident voordoet'.

Deze stellingen werden opnieuw gekruist met de achtergrondvraag 'Hoeveel medewerkers werken er ongeveer in de onderneming?'. Er werd bij alle drie de stellingen een statistisch significant verband vastgesteld. Bij de eerste twee stellingen vonden we een zwak verband indien dit gekruist werd met het aantal medewerkers. Bij de laatste stelling 'Er is een plan van aanpak aanwezig voor als er zich een beveiligingsincident voordoet' vonden we een redelijk of matig verband terug. De ondernemingen die het vaakst 'helemaal niet akkoord' tot 'eerder niet akkoord' waren, betroffen de kleinste, namelijk deze waarin 0 tot 10 medewerkers zijn tewerkgesteld. De grotere ondernemingen (vanaf meer dan 251 medewerkers) antwoordden vaker 'eerder akkoord', 'wel akkoord' of 'helemaal wel akkoord'.

Tot slot werd binnen het thema veiligheidscultuur, management en beleid inzake beveiliging in de onderneming gepolst welke actor of instantie een taak heeft in de strijd tegen criminaliteit.



Figuur 7: De veiligheid in de strijd tegen criminaliteit is een taak van: (N=146)

Bovenstaande top 6 toont aan dat diegene die beschouwd wordt als de belangrijkste verantwoordelijke voor de veiligheid in de onderneming de werkgever is. Vervolgens werd de overheid aangeduid, evenals de politie. Op de vierde plaats kwam 'iedere werknemer in onze onderneming', vervolgens de beroepssector zelf en als laatste de private veiligheidssector. Deze percentages zijn gebaseerd op de percentages respondenten die 'helemaal wel akkoord' tot 'akkoord' antwoordden.

Deze cijfers bevestigen de reeds aangegeven conclusie dat de werkgever verantwoordelijk wordt geacht voor de beveiliging van een onderneming.

3.5 IT-beveiliging is belangrijk in een onderneming

Op de vraag hoe belangrijk IT-beveiliging is in de onderneming antwoordde 93,84% van de respondenten 'helemaal wel belangrijk' tot 'belangrijk'. De ondernemingen met meer dan 11 medewerkers hebben het vaakst 'helemaal wel belangrijk' aangeduid.

82,19% stelde dat er iemand in de onderneming bezig is met IT-beveiliging. Het kruisen van deze vraag met het aantal medewerkers leverde een redelijk of matig significant verband op. De grote ondernemingen antwoordden doorgaans positief, terwijl de ondernemingen met 0 tot 10 medewerkers het vaakst aangaven dat er niemand bezig is met de IT-beveiliging in de onderneming.

72,6% gaf aan dat de onderneming een specifiek beveiligingsbeleid heeft op IT-niveau. De grote ondernemingen antwoordden positiever op deze vraag, terwijl de zeer kleine ondernemingen (0-10 medewerkers) het vaakst negatief antwoorden.

82,19% stelde dat er een beveiligingssysteem is in de onderneming. De grote ondernemingen antwoordden overtuigender 'ja'.

De vraag 'Wat was het budget voor IT-beveiliging dit jaar in vergelijking met vorig jaar?' genereerde de volgende resultaten:

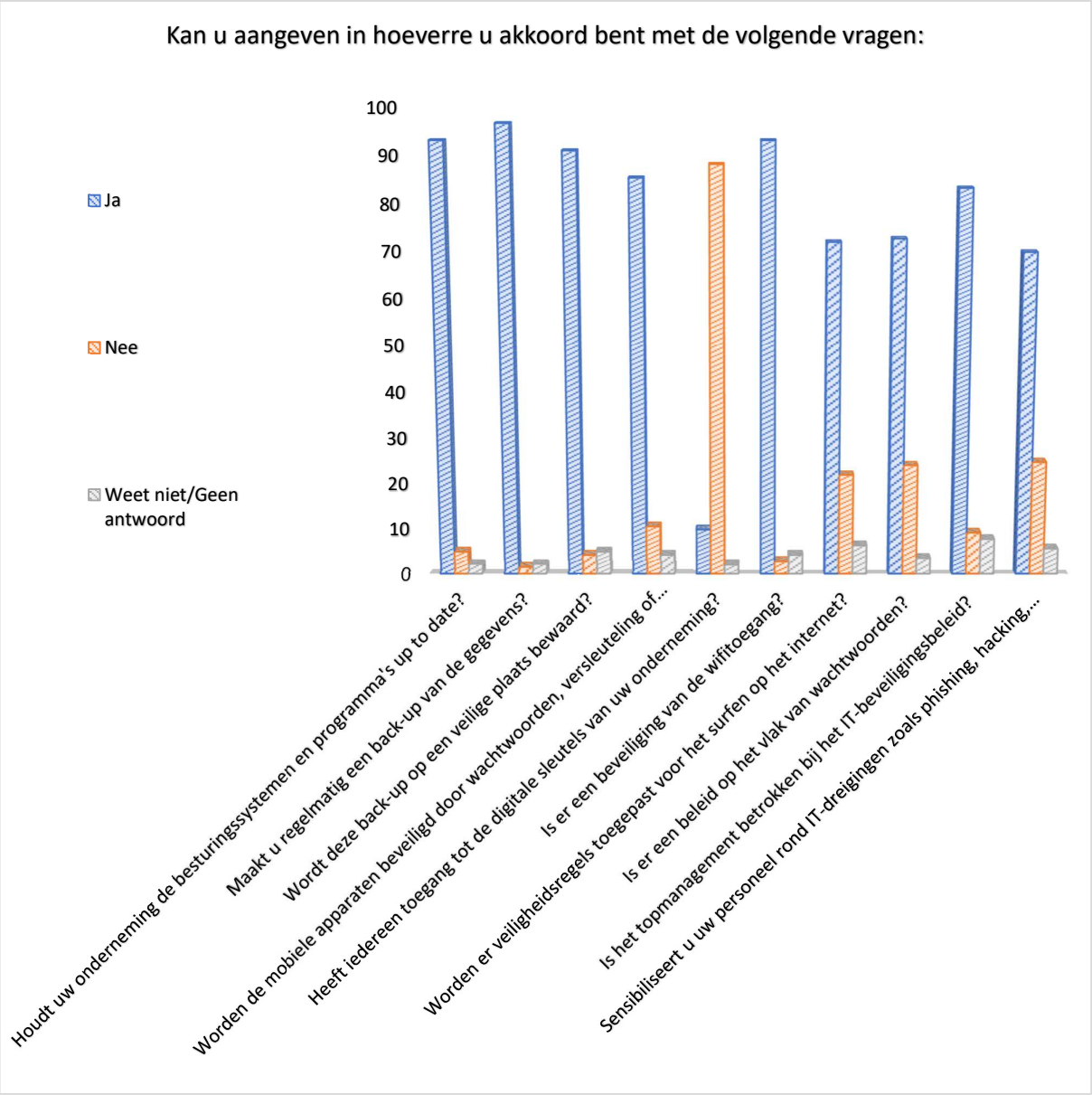
- 26,03%: het bleef hetzelfde
- 23,97%: ik heb geen kennis over het budget
- 23,29%: het verhoogde een beetje
- 19,18%: het verhoogde veel
- 6,16%: ik weet niet of het budget verhoogde
- 1,35%: het was minder dan het voorbije jaar

Iets meer dan de helft van de respondenten antwoordde 'ja' op de vraag 'Krijgt u of krijgen andere werknemers in uw onderneming een training over beveiliging en actuele bedreigingen op IT-niveau?'. 44,52% stelde dat

dit niet het geval is. Een statistisch significant verband met de grootte van de onderneming werd gevonden: bij de kleine ondernemingen zijn er weinig mensen die aangeven dat zij regelmatig een opleiding krijgen over de beveiliging of actuele bedreiging op IT-niveau.

De verhoogde aandacht en budgetten voor IT-beveiliging zijn noodzakelijk in de huidige, technologische samenleving. Op die manier kan slachtofferschap vermeden worden, evenals reputatieschade. Ondernemingen worden evenzeer verplicht om zorgvuldig om te springen met data. Sinds de wijziging van de privacywet van 1992 in de General Data Protection Regulation (2018) kunnen immers boetes opgelegd worden als deze niet gerespecteerd wordt (Hoeffnagel, 2016).

Vervolgens werden enkele beveiligingsvragen gesteld, gebaseerd op een aantal vuistregels opgesteld door de FOD Economie (2017) over de IT-beveiliging in een onderneming.



Figuur 8: Kan u aangeven in hoeverre u akkoord bent met de volgende vragen: (N=142)

96,48% maakt regelmatig een back-up van de gegevens. Slechts 1,41% doet dit niet en 2,11% gaf geen antwoord op deze vraag of wist het niet. 92,96% gaf aan dat de onderneming de besturingssystemen en programma's up-to-date houdt. Op de vraag of de back-up op een veilige plaats wordt bewaard, antwoordde 90,85% positief. 92,96% gaf aan dat er een beveiliging is van de wifitoegang. Volgens 88,03% heeft niet iedereen toegang tot de digitale sleutels van de onderneming. Het topmanagement is volgens 83,1%

betrokken bij het IT-beveiligingsbeleid, volgens 9,16% is dit niet het geval en 7,75% beantwoordde deze vraag niet of wist het niet. Op de vraag 'Worden de mobiele apparaten beveiligd door wachtwoorden, versleuteling of blokkering vanop afstand' poneerde 85,21% dat dit het geval is, 10,56% stelde dat dit niet het geval is en 4,23% wist het niet of beantwoordde deze vraag niet.

72,54% gaf aan dat er een beleid is op het vlak van wachtwoorden, terwijl 23,94% aangaf dat dit niet het geval is. 3,52% wist het niet of gaf geen antwoord. Op de vraag of er veiligheidsregels worden toegepast voor het surfen op internet antwoordde 21,83% van niet, 71,83% van wel en 6,34% gaf geen antwoord op deze vraag of wist het niet. Op de vraag 'Sensibiliseert u uw personeel rond IT-dreigingen zoals phishing, hacking, …?' antwoordde 69,72% positief, 24,65% negatief en 5,63% wist het niet of kon geen antwoord geven.

In de Aons' Global Risk Management Survey van 2017 werd niet alleen ingegaan op de top 10 van risico's maar werd ook gevraagd in hoeverre men voorbereid is op het voorvallen van risico's, de zogenaamde 'risk-preparedness'. Gezien cybercrimes aanzienlijk stijgen in kostprijs en het langer duurt vooraleer ze worden opgelost, is het cruciaal dat bedrijven klaar zijn voor een cybercrime. De meerderheid van de bedrijven geeft aan dat ze zich hierop voorbereiden door middel van plannen over hoe om te gaan met risico's. Er wordt in dit onderzoek gerapporteerd dat 79% klaar is voor cybercrime/hacking/viruses/malicious codes. Dit percentage 'readiness' is het hoogste in vergelijking met de percentages bij alle andere misdrijven (Aons' Global Risk Management Survey, 2017).

In 2017, bevroeg Tech Pro Research IT-professionelen over hun *"companies' cybersecurity readiness in the face of threats presented by mobile and IoT-connected devices"*. Enkele van hun belangrijkste bevindingen waren:

- De meerderheid van de respondenten (39%) gaf zijn of haar bedrijf een score boven het gemiddelde op het vlak van cybersecurity readiness.
- Bijna de helft van de respondenten (49%) stelde dat deze readiness verbeterde het laatste jaar. Slechts 8% gaf aan dat deze bereidheid daalde.
- Van alle cyberveiligheidsrisico's stelden de respondenten dat hun bedrijf het meest bedreigd werd door phishing, ransomware en virussen.
- De meest gebruikelijke methodes om cybersecurity te implementeren zijn het gebruik van malware producten, toepassen van patches en updates en het aannemen van fysische veiligheidsmethodes;
- De drie meest populaire technieken voor het creëren van een cybersecuritycultuur waren gebruikseducatie, IT-personeel en veiligheidsgerelateerde aankondigingen.

Tech Pro Research onderzocht in 2018 welke cyberveiligheidsstrategie ondernemingen hebben. Er werden 236 professionelen bevraagd over hun strategie inzake cyberveiligheid. Er werd evenzeer ingegaan op de vraag hoe men deze strategie omzet in de praktijk. In het rapport 'Cybersecurity strategy research: Common tactics, issues with implementation, and effectiveness' van 2018 concludeerde Tech Pro Research:

- In het algemeen toonden de resultaten aan dat de meeste bedrijven meerdere tactieken gebruiken om zich te beschermen tegen schendingen en aanvallen, waardoor niemand tekort schiet op dit domein. De problemen liggen hem echter in het implementeren van de veiligheidsmaatregelen.
- Veel respondenten stelden dat de werknemersvereniging een struikelblok was, en minder, maar nog steeds een significante groep van respondenten zei dat het leiderschap en het krijgen van adequate fondsen de uitdagingen zijn. Tot slot gaf de meerderheid van de bevraagde respondenten door Tech Pro Research aan dat zij iets of matig vertrouwd zijn met de mogelijkheden die een onderneming heeft om zich te beschermen tegen cybercriminaliteit.

Op het niveau van Europese data vinden we deze Belgische statistieken terug in Eurostat. In een rapport over ICT security in enterprises wordt hier op ingegaan. De data werden verzameld op basis van de *Community Survey on ICT usage and e-commerce in enterprises*[2] uit 2015. In deze context verwijst ICT-security naar de relevante incidenten en de maatregelen, controles, procedures die toegepast worden door bedrijven zodat ze de integriteit, confidentialiteit en beschikbaarheid van hun data en ICT-systemen kunnen verzekeren. De vraag werd gesteld aan de bedrijven hoezeer zij een formeel ICT-security beleid hebben. Als men kijkt naar de EU 28 (de EU in haar huidige samenstelling), zien we dat 32% van alle bedrijven aangaf een formeel ICT-security beleid te hebben. Dit betekent dat ongeveer één derde van de bedrijven een ICT-veiligheidsbeleid heeft op

[2] Deze data zijn gebaseerd op cijfers van 2015. Ongeveer 148800 ondernemingen, met meer dan 10 werknemers, van de 1.5 miljoen in de EU 28 werden bevraagd. Van deze 1.5 miljoen bedrijven wordt geschat dat ongeveer 83% van de bedrijven tussen de 10 en 40 medewerkers tewerkstelt, 14% tussen de 50 en de 249 medewerkers en 3% meer dan 250 medewerkers.

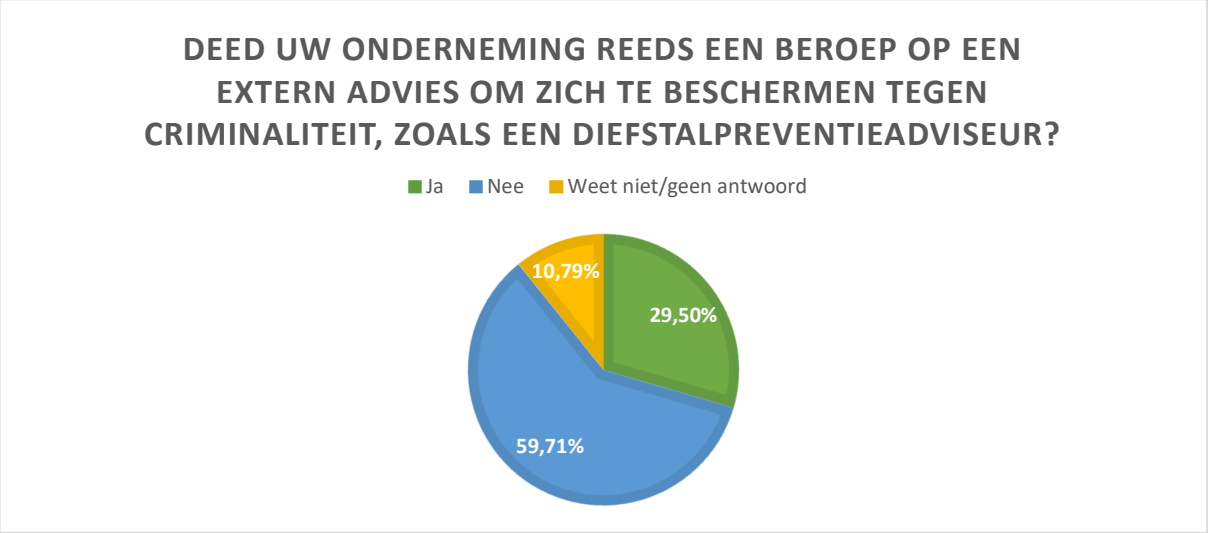
dit domein. Als we inzoomen op het Belgische percentage is dit evenzeer 32% van de bevraagde Belgische bedrijven. Er wordt een onderscheid gemaakt tussen grote, medium en kleine bedrijven. Van de grote[3] bedrijven gaf 72% aan dat zij een ICT-security beleid hebben, van de mediumbedrijven[4] stelde 51% een dergelijk beleid te hebben, terwijl dit in de kleine bedrijven 27% was[5].

783 leden van UNIZO werden in 2016 bevraagd rond cybercriminaliteit en andere vormen van criminaliteit (UNIZO, 2016). 7/10 van de bevraagden neemt zelf beveiligingsmaatregelen. 43% beschikt over uitgebreide beveiligingstools, zoals een degelijk back-up systeem, een firewall, antivirus software, … 30% besteedt haar IT-beveiliging uit aan een IT-partner of een beveiligingsbedrijf. Van deze 30% stelt 10% dat zij niet op de hoogte is van het soort maatregelen die de IT-leverancier levert.

UNIZO stelt vast dat er enerzijds ondernemingen zijn die zich in erg of vrij beperkte mate beveiligen en anderzijds zijn er ondernemingen die veel investeren in de beveiliging. Deze laatste ondernemingen, die veel contacten onderhouden met de IT-partner die hun onderneming beveiligt, zouden minder last hebben van cybercriminaliteit. UNIZO pleit ervoor dat iedere onderneming zich de vraag stelt hoe men zich beter kan beschermen en wat men moet doen om zich te beschermen. Er wordt waakzaamheid gevraagd ten aanzien van alle vormen van criminaliteit op internet.

3.6 Fysieke en organisatorische beveiliging

Naast de mate waarin een onderneming bezig is met IT-beveiliging, werden ook enkele vragen gesteld over de fysieke en organisatorische beveiliging.



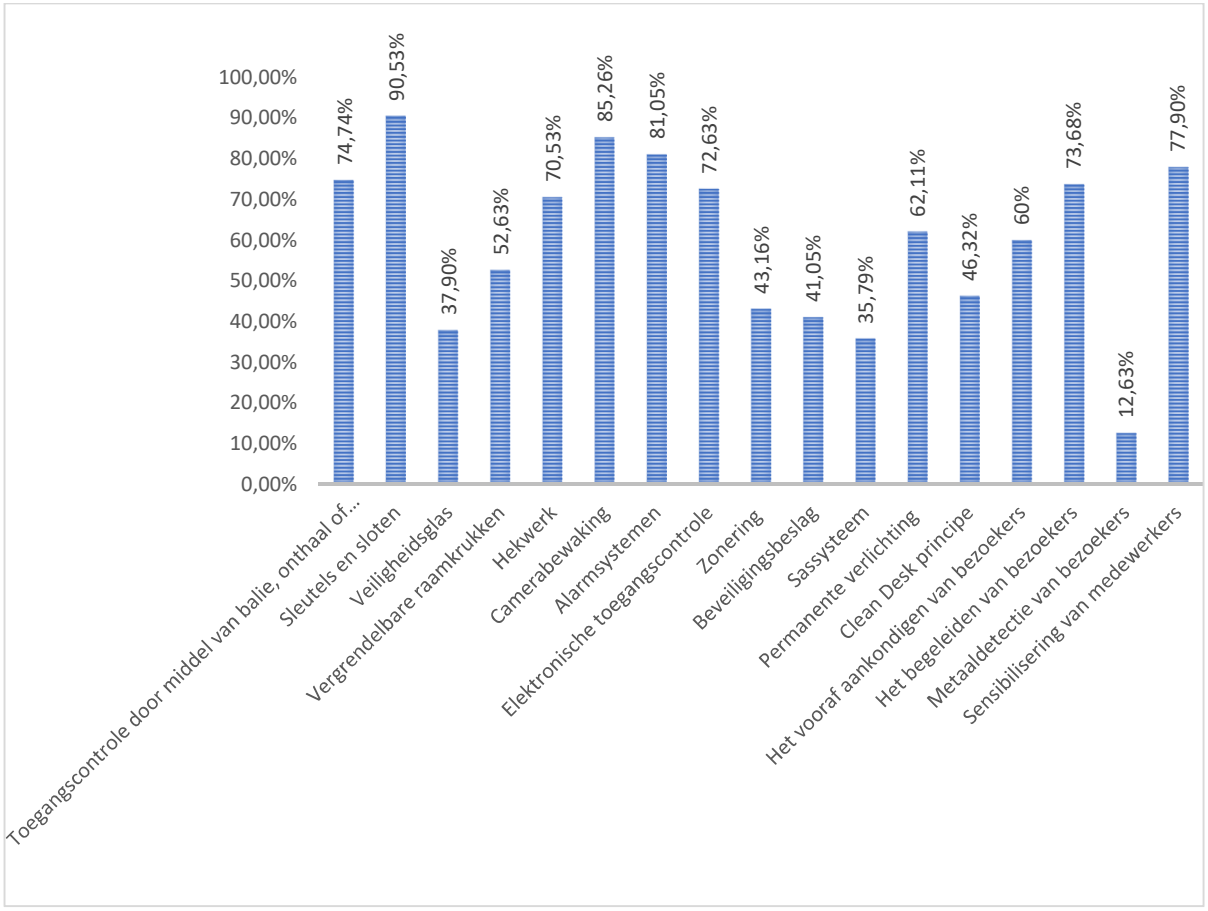
Figuur 9: Deed uw onderneming reeds een beroep op een extern advies om zich te beschermen tegen criminaliteit? (n=139)

Zoals men kan aflezen in figuur 9, gaf 60% van de bevraagden aan dat hun onderneming nog geen beroep deed op een extern advies om zich te beschermen tegen criminaliteit. Een kleine 30% antwoordde 'ja' en 10,79% antwoordde 'weet niet' of gaf geen antwoord.

Op de vraag of de onderneming reeds in één of meerdere systemen investeerde om zich fysiek of organisatorisch te beveiligen (bijvoorbeeld tegen criminaliteit) antwoordde 69,07% positief en 24,46% negatief. 6,48% gaf geen antwoord of wist het niet.

De respondenten die 'ja' antwoordden, kregen allerhande vormen van fysieke of organisatorische beveiliging voorgelegd, zoals in de onderstaande figuur af te lezen is.

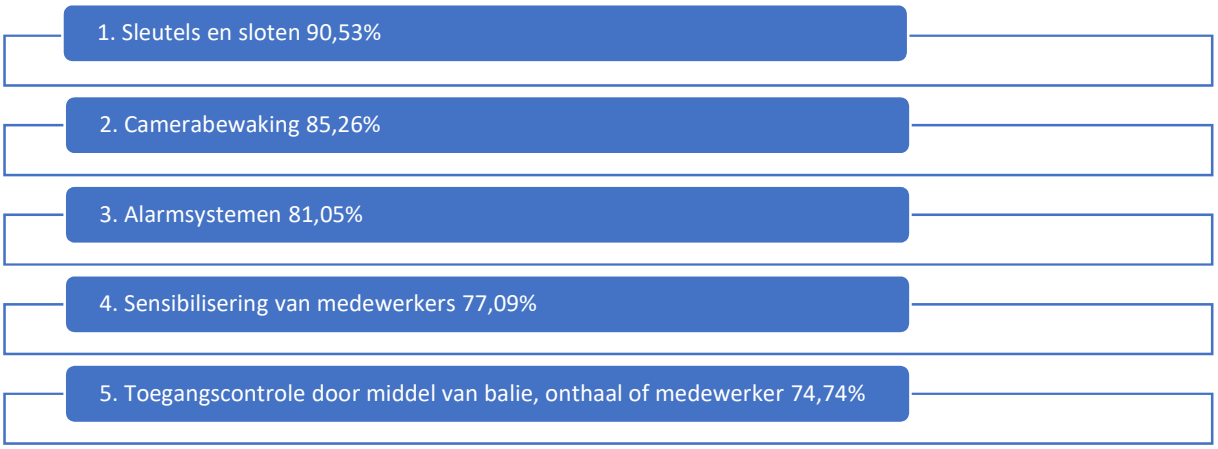
[3] Dit zijn bedrijven waarin meer dan 250 personen tewerkgesteld zijn.
[4] Dit zijn bedrijven waarin 50 tot 249 personen tewerkgesteld zijn.
[5] Een klein bedrijf betreft een bedrijf die 10 tot 49 personeelsleden tewerkstelt.



Figuur 10: Percentage respondenten dat 'ja' antwoordde op de vraag 'Investeerde uw onderneming reeds in één of meerdere systemen om zich fysiek of organisatorisch te beveiligen (bijvoorbeeld tegen criminaliteit)'? (N=95)

De respondenten die aangaven dat de onderneming investeerde in fysieke of organisatorische beveiliging duidden in hoofdzaak de volgende vormen aan: toegangscontrole door middel van balie of onthaal (74,74%), sleutels en sloten (90,53%), hekwerk (70,53%), camerabewaking (85,26%), alarmsystemen (81,05%), elektronische toegangscontrole (72,63%), permanente verlichting (62,11%), het vooraf aankondigen van bezoekers (60%), het begeleiden van bezoekers (73,68%) en het sensibiliseren van medewerkers (77,90%).

Figuur 11: Top 5 van meest courante vormen van fysieke of organisatorische beveiliging (N = 95)



Opvallend aan deze resultaten is dat de traditionele beveiligingsmethoden in hoge mate aanwezig zijn. De hoge percentages bij de categorieën sleutels en sloten (90,53%) en toegangscontrole door balie of onthaal (74,74%) beamen dit.

De investering die het minst werd aangeduid is 'metaaldetectie van bezoekers'. Slechts 12,63% van de respondenten duidde dit aan. De personen die 'andere' aanduidden als beveiligingssysteem gaven doorgaans de volgende antwoorden: badgesysteem om specifieke toegangen te krijgen, elektronische bewaking en specifieke toegangscontrolesystemen met hightech solutions, camera, hond, …

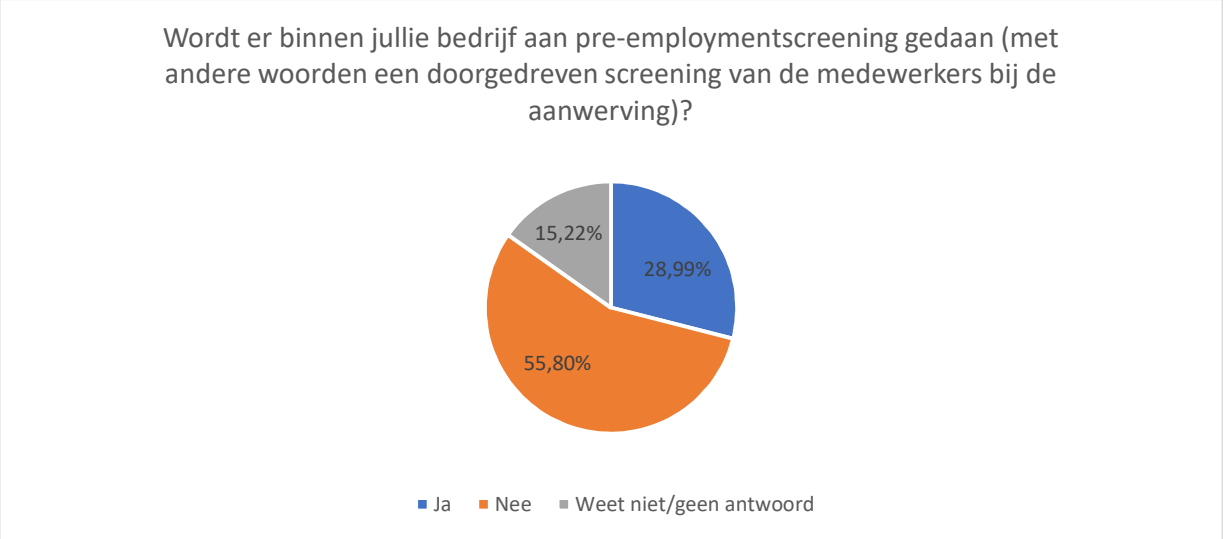
In de UNIZO-bevraging (UNIZO, 2016) werden evenzeer enkele vragen gesteld aangaande algemene beveiliging. 68% van de bevraagden investeerde reeds in één of meerdere beveiligingssystemen. De helft gaf aan een alarmsysteem te hebben geïnstalleerd en de helft wenste betrokken te worden bij een Buurt Informatie Netwerk (11% was reeds lid van een BIN).

Bij het kruisen van de vragen die peilen naar de aanwezigheid van één of meerdere systemen om zich fysiek of organisatorisch te beveiligen met het aantal medewerkers in een onderneming vonden we enkele significante verbanden.

We vonden een sterk statistisch significant verband tussen het aantal medewerkers en het gebruik van camerabewaking en toegangscontrole door middel van een balie, onthaal of medewerker. Hoe groter de onderneming, hoe vaker deze maatregelen werden aangeduid.

Daarnaast vonden we een aantal redelijke of matige statistisch significante verbanden tussen de grootte van de onderneming en het investeren in bepaalde maatregelen. Zo antwoordden bedrijven tot en met 250 medewerkers vaker 'nee' op de vraag of ze veiligheidsglas gebruiken. Ook het gebruik van vergrendelbare raamkrukken, elektronische toegangscontrole, een sassysteem, permanente verlichting of een 'clean desk'-principe komen vaker voor in grote dan in kleine bedrijven. Het niet vooraf aankondigen en niet begeleiden van bezoekers komen het vaakst voor in ondernemingen met slechts 0-10 medewerkers. Over het gebruik van een alarmsysteem, ten slotte, was er verdeeldheid.

3.7 Screening van het personeel



Figuur 12: Wordt er aan pre-employmentscreening gedaan? (N=138)

Iets meer dan de helft van de respondenten (namelijk 55,8%) antwoordde 'nee' op de vraag of er aan pre-employmentscreening wordt gedaan. 28,99% gaf aan dat dit wel het geval is en 15,22% wist het niet of gaf geen antwoord op deze vraag. Aan de respondenten die 'ja' antwoordden, werd gevraagd of deze screening gebeurt voor alle functies, wat door 75% werd beaamd. 15% stelde dat de screening enkel gebeurt voor veiligheidsspecifieke functies en 5% antwoordde 'nee'. In een volgende vraag werden aspecten opgesomd die kunnen gescreend worden. Datgene dat het meest gescreend wordt, zijn 'actieve check referenties' (positief beantwoord door 85% van de respondenten), 'blanco's in CV controleren' (82,5% antwoordde 'ja'), 'contact met vorige werkgever' (75% bevestigde dit) en 'sociale media doorzoeken' (65% antwoordde positief). 'Andere

open bronnen raadplegen (bv. Belgisch Staatsblad)', ten slotte, werd bevestigd door 50% van de respondenten. 27,5% stelde dat men voor deze screening een extern bureau inschakelt.

De respondenten die aangaven dat er een pre-employmentscreening gebeurde door hun bedrijf, werden gevraagd of deze screening ook door andere instanties gebeurt. Iets meer dan 60% van de respondenten gaf aan van wel. 30% stelde van niet en 7,5% wist het niet of gaf geen antwoord. Er werd tevens gevraagd of er aan in-employmentscreening wordt gedaan tijdens de loopbaan, zoals het herevalueren en screenen van bestaande werknemers na verloop van tijd. 60,29% antwoordde 'nee', 30,88% antwoordde 'ja' en 8,82% wist het niet of gaf geen antwoord.

Vandaag is een screening aan de hand van allerlei sociale mediakanalen zoals Facebook, Twitter en Linkedin snel gebeurd, wat wordt bevestigd door Bafort (2016). Zo bleek bijvoorbeeld dat een kandidaat met een gunstige profielfoto tot 21% meer positieve reacties kreeg op zijn sollicitatie in vergelijking met een kandidaat met een minder gunstige profielfoto (Bafort, 2016).

3.8 Slachtofferschap

3.8.1 Ondernemingen werden de laatste 12 maanden het vaakst slachtoffer van cybercriminaliteit

Een belangrijk onderdeel van deze bevraging was de module 'slachtofferschap', waarin gevraagd werd of de onderneming de laatste 12 maanden slachtoffer is geweest van een bepaald feit.

In wat volgt sommen we de minst frequent aangeduide feiten op waar de onderneming of een medewerker van de onderneming slachtoffer van werd tijdens de laatste 12 maanden:

Terrorisme (2,94% werd slachtoffer)
Mensensmokkel/-handel (5,88% werd slachtoffer)
Witwassen (5,88% werd slachtoffer)
Diefstal gewapenderhand (7,35% werd slachtoffer)
Chantage of afpersing (niet via internet) (8,82% werd slachtoffer)
Cybercriminaliteit: cyberafpersing (9,56% werd slachtoffer)
Ongeoorloofde toegang met geweld (9,56% werd slachtoffer)
Sabotage (11,03% werd slachtoffer)
Cybercriminaliteit: internetfraude (11,77% werd slachtoffer)

Tabel 3: Is uw onderneming of een medewerker van uw onderneming in dienstverband slachtoffer geweest de laatste 12 maanden van (N=136)

Terrorisme, mensensmokkel/-handel en witwassen zijn de minst frequent voorkomende feiten waar een onderneming slachtoffer van werd de laatste 12 maanden. Deze criminaliteitsfenomenen werden ook aangeduid in de vraag naar risico-inschatting. Hieruit bleek dat mensenhandel (83,89%), witwassen (83,33%), valse munten (76,11%) en terrorisme (75%) als het minst waarschijnlijk worden geacht om er slachtoffer van te worden.

In onderstaande tabel wordt de top 4 van feiten weergegeven waar de onderneming of een medewerker van de onderneming slachtoffer van werd tijdens de laatste 12 maanden:

		Ja	Nee	Weet niet/geen antwoord
1	Een van de 5 vormen van cybercriminaliteit	42,6%	53,7%	3,7%
2	Beschadiging van een voertuig (fiets, moto, auto, bestelwagen, vrachtwagen…)	41,91%	53,68%	4,41%
3	Geweld, agressie (zonder diefstal)	39,71%	55,15%	5,15%
3	Beschadiging van eigendom (geen voertuig) of vandalisme	39,71%	58,09%	2,21%
4	Ongeoorloofde toegang zonder geweld	38,24%	58,09%	3,68%

Tabel 4: Top 4 van feiten waar een onderneming of medewerker van een onderneming slachtoffer van werd de laatste 12 maanden (N=136)

Bijna 43% van de bevraagde ondernemingen duidde aan dat zij de laatste 12 maanden slachtoffer werden van één van de 5 voorgelegde vormen van cybercriminaliteit. 41,91% gaf aan dat zij slachtoffer werden van beschadiging aan een voertuig (zoals een fiets, moto, auto, bestelwagen, vrachtwagen) en 2% minder stelde dat een eigendom (geen voertuig) werd beschadigd of er vandalisme werd gepleegd tijdens de laatste 12 maanden. Een gelijkaardig percentage, namelijk 39,71%, vinden we terug voor geweld en agressie (zonder diefstal); dit betekent dat meer dan 1 op de 3 ondernemingen slachtoffer werd van geweld, agressie (zonder diefstal) of van een bepaalde vorm van beschadiging aan het voertuig of eigendom.

Als er ingezoomd wordt op de verschillende vormen van cybercriminaliteit, waren de twee meest voorkomende vormen:

		Ja	Nee	Weet niet/geen antwoord
1	Cybercriminaliteit: illegale toegang tot IT systemen (dmv hacking, phishing, gissen van een paswoord…)	33,09%	60,29%	6,62%
2	Cybercriminaliteit: tussenkomst in data of systemen (dmv virusssen, cryptoware, (D)Dos aanvallen door botnets)	29,41%	63,97%	6,62%

Tabel 5: Twee meest voorkomende vormen van cybercriminaliteit waar een onderneming of medewerker van een onderneming slachtoffer van werd de laatste 12 maanden (N=136)

De feiten uit tabel 4 en 5 werden gekruist met het aantal medewerkers dat tewerkgesteld is in de onderneming. Er werden verschillende significante verbanden gevonden, die doorgaans redelijk of matig van aard waren. Voor 'geweld, agressie (zonder diefstal)' zien we dat ondernemingen met meer dan 251 medewerkers hiervan frequenter slachtoffer werden. De criminaliteitsvorm 'diefstal van een voertuig (fiets, moto, auto, bestelwagen, vrachtwagen…)' levert evenzeer een statistisch significant verband op als dit gekruist wordt met het aantal medewerkers in de onderneming. De helft van de respondenten uit de ondernemingen waar tussen de 251 en 500 medewerkers of meer dan 1001 medewerkers werken, antwoordde 'ja' op deze vraag. Ondernemingen waar minder dan 250 medewerkers werken, antwoordden in 90% van de gevallen 'nee'.

Van 'diefstal gewapenderhand' werd men in de meerderheid van de gevallen geen slachtoffer, enkel de grote bedrijven met meer dan 1001 medewerkers gaven af en toe aan van wel. Een gelijkaardig resultaat vinden we bij de vorm 'diefstal met geweld – zonder wapen'.

De respondenten die de laatste 12 maanden slachtoffer werden van 'ongeoorloofde toegang met geweld' zijn gering en situeren zich in hoofdzaak in de grote ondernemingen. Bij de vraag waarin gepeild werd naar beschadiging van voertuigen (fiets, moto, auto, bestelwagen, vrachtwagen…) werd er verdeeld geantwoord. Voornamelijk ondernemingen met tussen de 251 en 1000 medewerkers gaven aan slachtoffer te zijn van dit feit. Ondernemingen waarin meer dan 501 medewerkers zijn tewerkgesteld werden frequenter slachtoffer van 'beschadiging van een eigendom (geen voertuig) of vandalisme'.

Het zijn voornamelijk de grote ondernemingen (met meer dan 1001 medewerkers) die de laatste 12 maanden slachtoffer werden van 'een vorm van fraude (sociale, fraude inzake afvalbeheer…), die niet via internet gepleegd wordt'. Gelijkaardige onderzoeksresultaten vinden we terug bij 'bedrog of oplichting (niet via internet)' en 'sabotage'.

Bij 'valse munten' ontstaat een statistisch significant verband: de kleine en middelgrote bedrijven (tot 500 medewerkers) antwoordden vaker 'nee' op de vraag of zij de laatste 12 maanden slachtoffer werden van deze criminaliteitsvorm. Ongeveer 43% van de ondernemingen waarin meer dan 1001 medewerkers actief zijn werd slachtoffer van 'valse of vervalste documenten'. De kleinere bedrijven geven doorgaans aan dat zij hier geen slachtofferschap ervaarden.

Ook wat betreft cybercriminaliteit werd naar verschillende vormen van slachtofferschap gepeild. Voor het slachtofferschap in de laatste 12 maanden van 'cybercriminaliteit: illegale toegang tot IT-systemen (dmv. hacking, phishing, gissen van een wachtwoord…)' werd een statistisch significant verband gevonden indien dit gekruist werd met het aantal medewerkers. Bedrijven van diverse groottes werden hier wel eens slachtoffer van, maar de bedrijven met meer dan 1001 medewerkers duidden dit het vaakst aan. We vonden een gelijkaardig onderzoeksresultaat bij 'cybercriminaliteit: tussenkomst in data of systemen (dmv. virussen, cryptoware, (D) Dos aanvallen door botnets)' en 'cybercriminaliteit: internetfraude'.

In het geval van 'cybercriminaliteit: cyberafpersing' werd de meerderheid hier geen slachtoffer van. In de weinige gevallen dat dit werd aangeduid, betrof dit ondernemingen met meer dan 1001 medewerkers.

Tot slot werd een statistisch significant verband gevonden tussen 'druggerelateerde feiten (handel, gebruik)' en het aantal medewerkers in de onderneming. Ongeveer 40% van de bedrijven met meer dan 501 medewerkers duidde aan dat zij hier slachtoffer van werden de laatste 12 maanden.

783 leden van UNIZO werden in 2016 bevraagd rond cybercriminaliteit en andere vormen van criminaliteit (UNIZO, 2016). 49,8% kreeg te maken met een vorm van cybercriminaliteit in 2016, wat een stijging betrof ten opzichte van 2014 en 2015 (ongeveer 40% en 30%).

In 15% van de gevallen ging het om IT-systemen die werden gehackt. Enkele ondernemers hadden problemen bij betalingen die werden uitgevoerd via internet en 23% stelde slachtoffer te zijn geweest van phishing. In de politionele geregistreerde criminaliteitscijfers staat cybercriminaliteit omschreven als een geografisch onafhankelijk fenomeen (Federale politie, 2016). Er zijn geen verschillen naargelang de aard van het bedrijf (cfr. economische sector). De federale politie geeft aan dat de schade per feit toeneemt, waarbij de vormen van cybercriminaliteit dermate evolueren en ondernemingen een belangrijker doelwit worden in vergelijking met particulieren.

Verder bevroeg UNIZO ondernemers over enkele aspecten aangaande veiligheid. Zo werd 10% van de 783 bevraagden het voorbije jaar slachtoffer van een inbraak/diefstal. Dit gebeurde in de meeste gevallen bij kleinhandelaars (23%) en in de bouwsector (16%). Ongeveer 30% werd ooit slachtoffer van een bepaalde vorm van agressie: dit betrof doorgaans verbale agressie.

Naar aanleiding van de terreurdreiging werd ook gevraagd of er enige bezorgdheid was bij de bevraagden hieromtrent. Zo bleek bijna de helft zich zorgen te maken na de aanslagen en gaf dit bij een kwart van de bevraagden aanleiding tot meer investeringen in veiligheid (UNIZO, 2016).

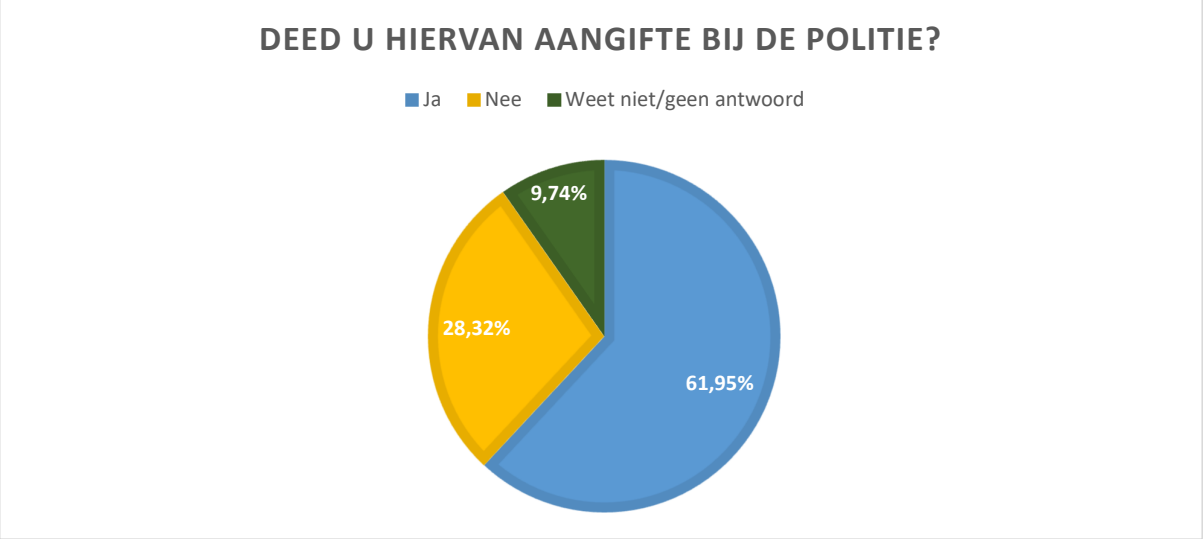
3.8.2 Geweld, agressie zonder diefstal is meest ingrijpende feit

Indien de onderneming of een medewerker van de onderneming één van bovenstaande vormen van criminaliteit meemaakte, werd de vraag gesteld welke van deze feiten het meest ingrijpend was. De slachtoffers duidden hierbij het vaakst de volgende feiten aan: 'geweld, agressie zonder diefstal' (19,3%), 'cybercriminaliteit: illegale toegang tot IT-systemen (dmv. hacking, phishing, gissen van een paswoord…)' (8,77%), 'ongeoorloofde toegang zonder geweld' (7,9%) en 'ladingdiefstal' (7,9%).

De redenen waarom een bepaald feit als ingrijpend werd beschouwd zijn velerlei: financieel, imago, persoonlijk, angst bij het personeel, … De hoogste percentages werden gevonden bij geweld, agressie zonder diefstal, omdat een individu daarbij persoonlijk getroffen wordt en dit als meest ingrijpend ervaart.

3.8.3 Een derde doet geen aangifte bij de politie

De volgende vragen in de barometer gingen dieper in op het meest ingrijpende feit waar de onderneming of een medewerker van de onderneming slachtoffer van werd.



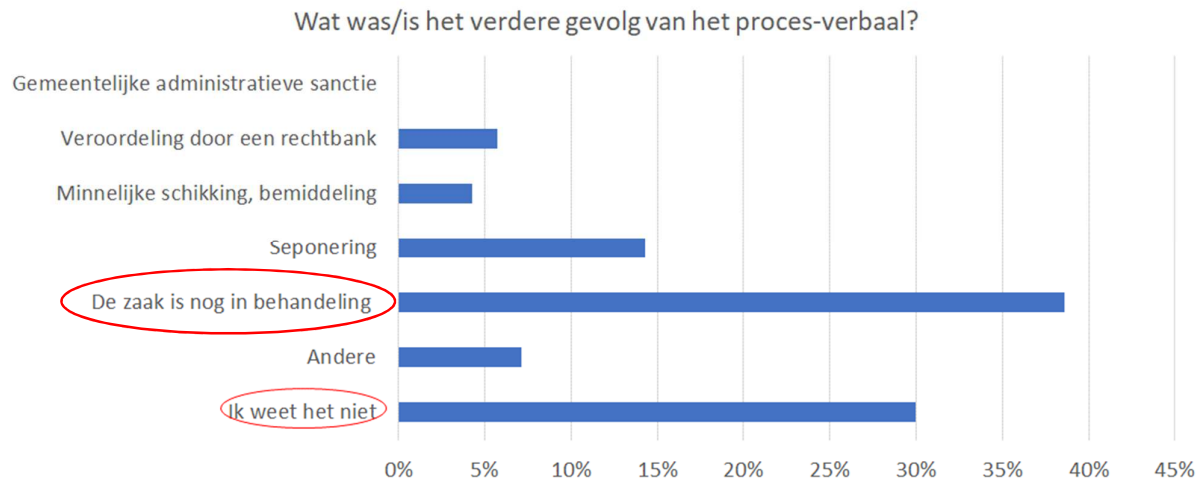
Figuur 13: Deed u hiervan aangifte bij de politie? (N=113)

Bij het interpreteren van bovenstaande figuur zien we dat 61,95% van de respondenten aangifte deed van de meest ingrijpende vorm van criminaliteit waarvan zij tijdens de laatste 12 maanden slachtoffer werd. Een derde van de bevraagde slachtoffers gaf aan van niet, en een kleine 10% wist het niet of gaf geen antwoord.

Wanneer deze vraag werd gekruist met het aantal medewerkers in de onderneming, werd een statistisch significant verband gevonden. De ondernemingen met een hoog aantal medewerkers antwoordden frequenter 'ja' in vergelijking met de middelgrote of kleine ondernemingen.

De hoofdredenen (opgelet bij de interpretatie van deze resultaten want de respondenten konden meerdere antwoorden geven) waarom men wel aangifte deed bij de politie zijn de volgende:

- Omdat dergelijke feiten in de toekomst voorkomen moeten worden (42,86%)
- Omdat we de zaak ernstig genoeg vinden (41,43%)
- Omdat de dader moet gepakt of gestraft worden (37,14%)
- Omdat we een bewijs voor de verzekering nodig hebben (34,29%)
- Omdat het een plicht is om te melden (22,86%)
- Omdat de politieorganisatie hier maatregelen tegen moet nemen (20%)



Figuur 14: Wat was/is het verdere gevolg van het proces-verbaal? (N=70)

Om eventuele verbanden te zien waarom men al dan niet aangifte deed, werd ook de vraag gesteld wat het verdere gevolg was van het proces-verbaal. Hierbij gaf 38,57% aan dat de zaak nog in behandeling is, terwijl 30% aangaf dit niet te weten. 14,29% antwoordde dat de zaak geseponeerd werd.

De slachtoffers die geen aangifte deden bij de politie werden evenzeer gevraagd wat de redenen hiertoe waren. De meest frequent gegeven redenen waren:

- Omdat dit toch geen resultaat oplevert (28,13%)
- Omdat we de dader kennen (15,63%)
- Andere (15,63%)
- Omdat we de zaak niet ernstig genoeg vonden (12,5%)
- Omdat er geen of weinig schade was (12,4%)
- Omdat men er toch niets kan aan doen (12,5%)

De bereidheid om een crimineel feit aan te geven is een cruciaal gegeven, en dit is niet alleen het geval voor België. Politiële criminaliteitsstatistieken worden bijgehouden en genereren een graadmeter of barometer van de geregistreerde criminaliteit. Dit laat de politie onder meer toe om op korte en lange termijn haar werking te evalueren of haar operationele werking bij te sturen (Federale politie, 2018). Bovendien kunnen beleidsmakers zich op deze cijfers baseren om een veiligheidsbeleid en -maatregelen uit te werken.

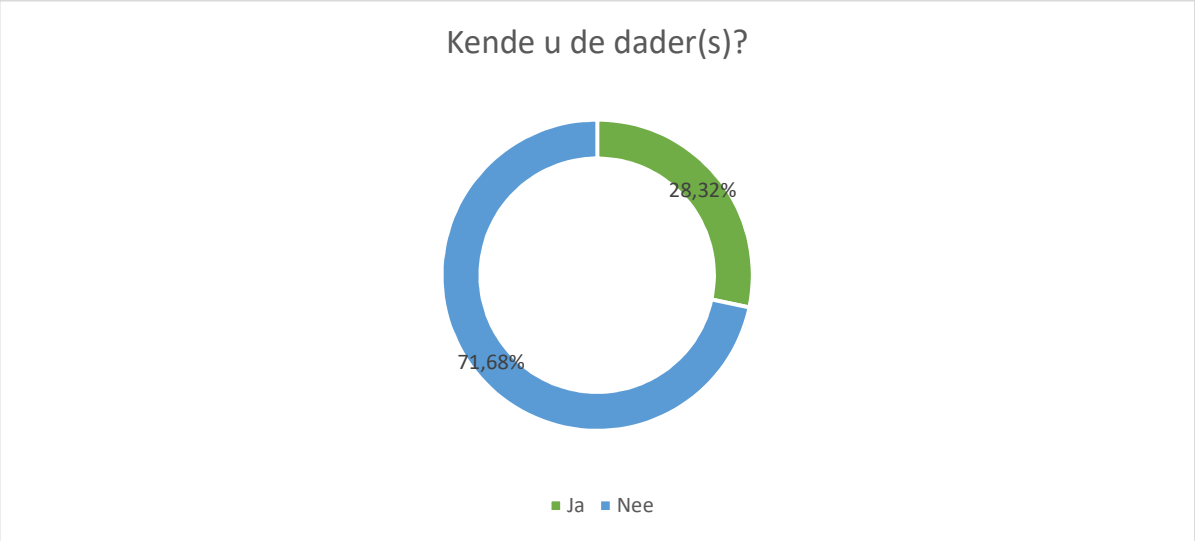
De politie kan enerzijds proactief optreden, de zogenaamde haalcriminaliteit, waarbij zij bijvoorbeeld zoekt naar criminaliteit door middel van acties of controles. Naast de haalcriminaliteit is er brengcriminaliteit waarbij slachtoffers aangifte doen (cfr. melding) en er een proces-verbaal wordt opgesteld. Gezien de beperkte capaciteit en middelen is de brengcriminaliteit de grootste bron van informatie. Het aangeven van criminaliteit is dus van groot belang (Versteegh, 2007), maar de praktijk toont aan dat dit geen sinecure is.

In de tendensen 2016-2017 van de federale politie wordt gewag gemaakt van de laagst opgetekende cijfers sinds het begin van de tellingen in 2000. Hier worden allerlei verklaringen voor gegeven zoals een 'International crime drop' : betere politiestrategieën en technieken, technopreventieve bescherming, toename van publieke camera's, private bewakingsfirma's… (van Dijk, Tseloni & Farrell, 2012). Deze dalende trend is een internationaal gegeven en vinden we ook terug in Nederland. Korpschef Akerboom stelde dat de Nederlandse politiecijfers in 2017 voor het vijfde jaar op rij daalden. Naast de International crime drop is het ook mogelijk dat er effectief minder criminaliteit wordt aangegeven door burgers. In een rapport 'Veilige buurt' werden verklaringen gezocht waarom slachtoffers feiten niet aangeven bij de politie. 39% van de respondenten verklaarde dit doordat 'dit toch geen zin had' (Veilige buurt, 2017).

De reden 'omdat dit toch geen resultaat oplevert' wordt in de literatuur beschreven als de rationele keuzebenadering. De kosten – zoals de moeite en bijkomende formaliteiten - worden afgewogen ten opzichte van de baten, wat in de perceptie van het slachtoffer 'niets' is. Deze rationele keuze speelt eveneens een rol bij de reden 'omdat we de dader kennen', waarbij feiten niet worden aangegeven omdat de schaamte en mogelijke wraakacties niet opwegen tegen de mogelijke gevolgen van de aangifte, zoals een potentiële vervolging. Er vindt met andere woorden een economische afweging plaats waarbij de baten niet opwegen tegen de kosten (Smets, De Kinder & Moor, 2011).

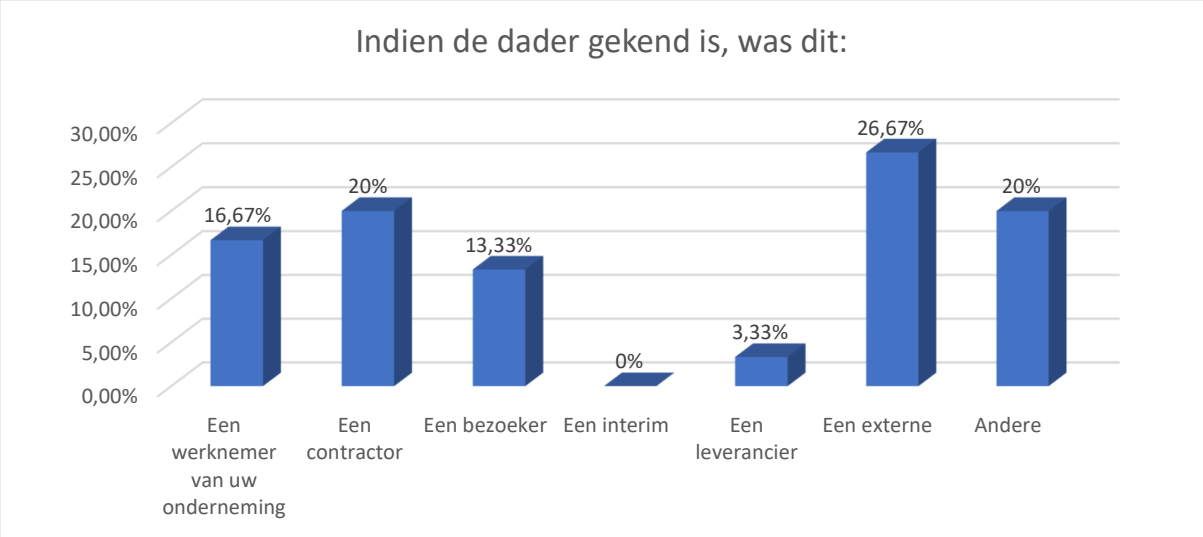
3.8.4 Eigenschappen van het crimineel feit

Aan diegenen die slachtoffer werden van een crimineel feit, werd gevraagd of men de dader ervan al dan niet kende. Zoals blijkt uit onderstaande figuur is het duidelijk dat 71,68% van de slachtoffers de dader niet kende, terwijl 28,32% de dader wel kende.



Figuur 15: Kende u de dader(s)? (N=113)

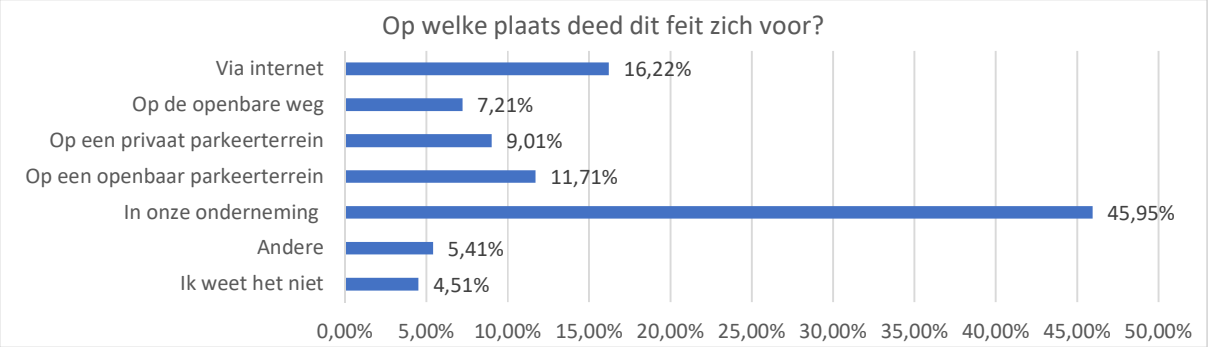
Indien de dader gekend is, werd de vraag gesteld wie dit was.



Figuur 16: Indien de dader gekend is, was dit: (N=30)

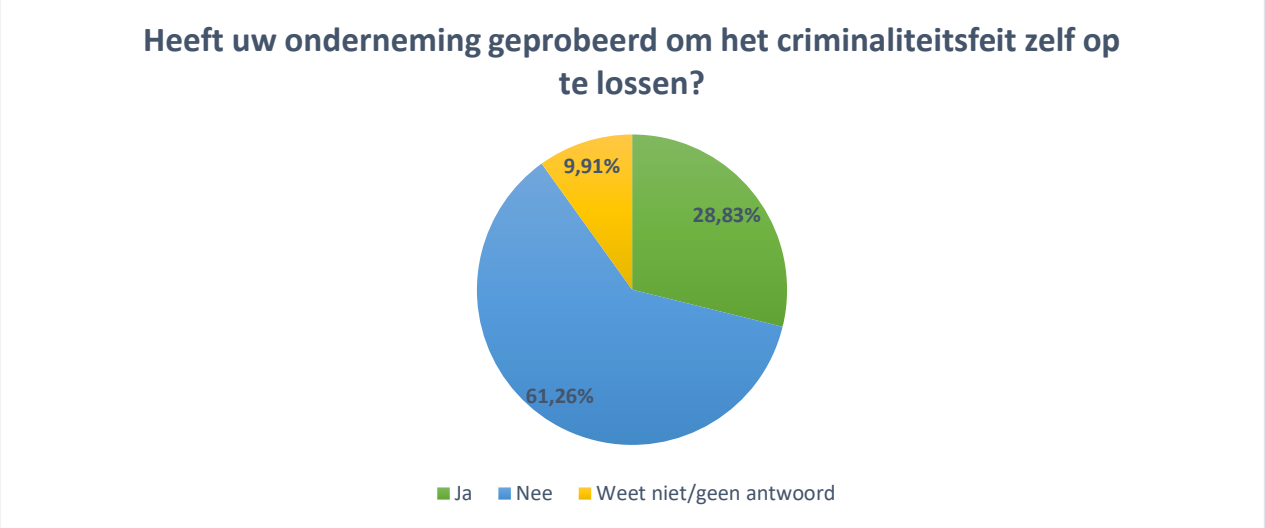
Figuur 16 geeft weer dat indien de dader gekend was, dit bij 26,67% van de respondenten een externe betrof, bij 20% een contractor of 'andere' en bij 16,67% een werknemer van de eigen onderneming.

Hoewel dit fenomeen weinig bestudeerd wordt, is er al lang een vermoeden dat de werknemerscriminaliteit toeneemt. Het begrip werknemerscriminaliteit is moeilijk definieerbaar en een frequent onzichtbaar probleem, waardoor de reikwijdte ervan onder de radar blijft. Het grootste deel van de werknemerscriminaliteit betreft vermogenscriminaliteit (Guinevere, 2010) maar ook andere vormen zijn in opmars. Zo bleek uit een recent onderzoek dat ruim één derde van de bedrijfsfraude gepleegd wordt door eigen personeel (De Tijd, 2018).



Figuur 17: Op welke plaats deed dit feit zich voor? (N=111)

In 45,95% van de gevallen deed het feit zich voor in de onderneming zelf. 16,22% werd slachtoffer van de criminele feiten via internet en 11,71% op een openbaar parkeerterrein.



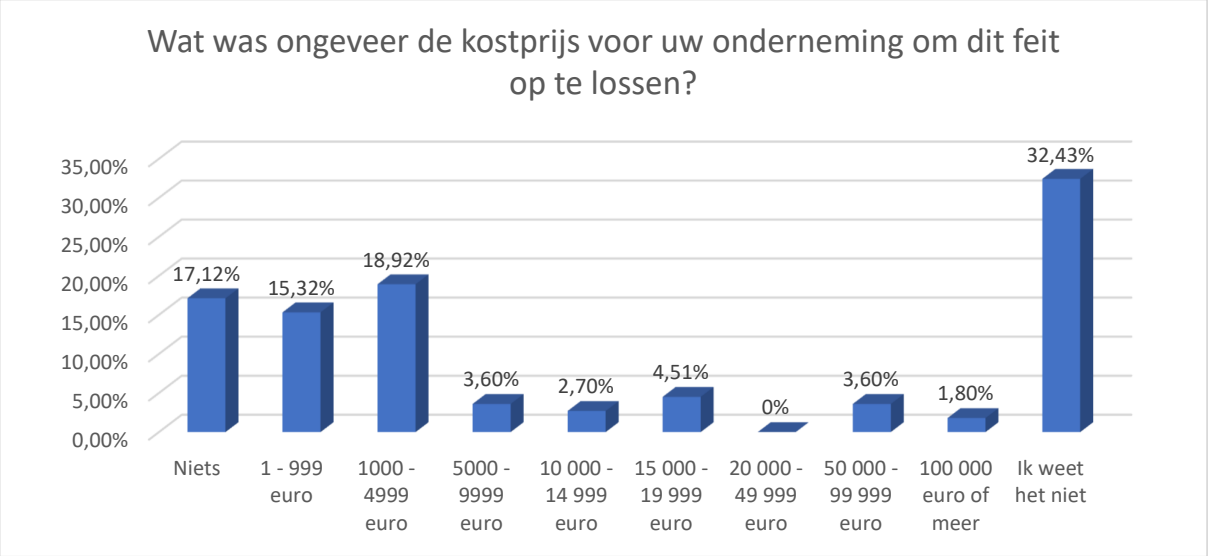
Figuur 18: Heeft uw onderneming geprobeerd om het criminaliteitsfeit zelf op te lossen? (N=111)

Op de vraag of de onderneming probeerde om het criminaliteitsfeit zelf op te lossen door bijvoorbeeld de dader te zoeken of aan te spreken, de schade in der minne te regelen, … merken we op basis van figuur 18 dat de meerderheid aangaf dat dit niet het geval was. Een derde van de respondenten (28,83%) stelde daarentegen dat dit wel gebeurde. In het onderzoek van Guinevere (2010) over werknemerscriminaliteit bleek dat 20% de baas verwittigt bij diefstal, 44% spreekt de werknemer aan, 44% zegt niets en 0% verwittigt de politie. Bedrijven doen in toenemende mate beroep op private opsporingsdiensten en/of richten interne onderzoeksafdelingen op om allerhande vormen van werknemerscriminaliteit tegen te gaan (WODC, 2010).

Indien we deze vraag kruisten met het aantal medewerkers in een onderneming leverde dit een statistisch significant verband op: ondernemingen tot 250 medewerkers antwoordden veel vaker 'nee' op de vraag: 'heeft uw onderneming geprobeerd om het criminaliteitsfeit zelf op te lossen (door bijvoorbeeld de dader zelf te zoeken of aan te spreken, de schade in der minne te regelen…)'.

Aan de slachtoffers werd vervolgens gevraagd hoeveel uren werktijd van het eigen personeel nodig waren om de criminaliteit zelf op te lossen. 33,33% antwoordde op deze vraag 'niet van toepassing', 18,02% gaf aan dat dit '1 uur tot een halve dag' was, 14,41% 'een halve dag tot een dag' en 13,51% 'minder dan 1 uur'. 11,71% stelde dat dit '1 week of meer' was.

Nog meer respondenten – namelijk 64,87% - antwoordden 'niet van toepassing' op de vraag hoeveel uren werktijd van een externe firma nodig waren om het criminaliteitsfeit op te lossen. Iets minder dan 10% stelde dat dit minder dan een uur was en 8,11% gaf aan dat dit 1 dag tot minder dan een week was.

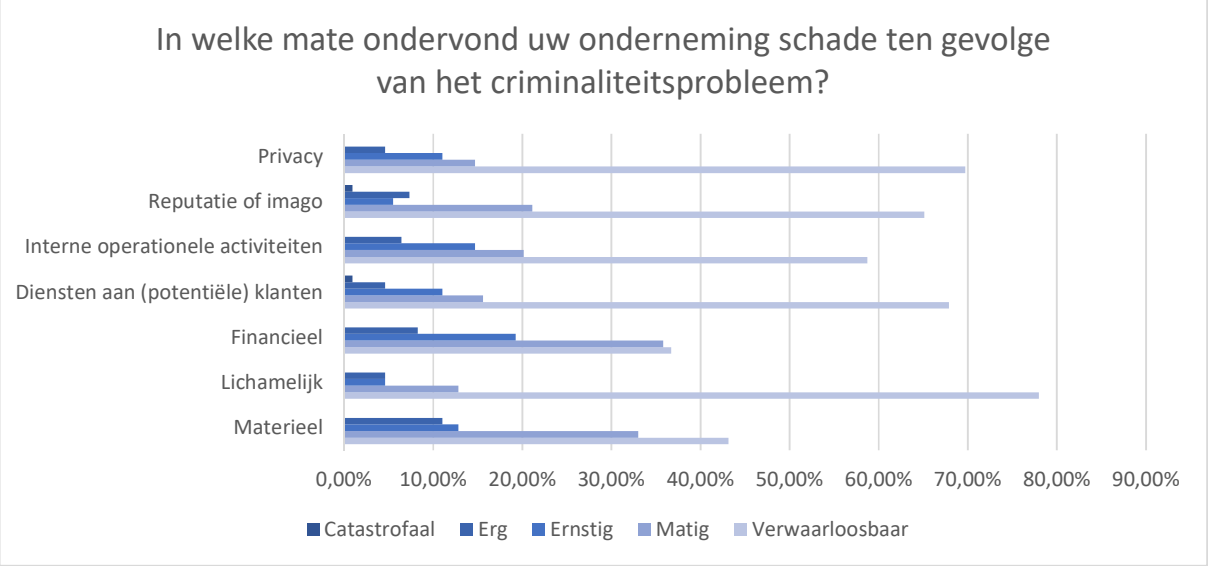


Figuur 19: Wat was ongeveer de kostprijs voor uw onderneming om dit feit op te lossen? (N=111)

Op de vraag wat de kostprijs was voor de onderneming om het feit op te lossen, antwoordde 32,43% 'ik weet het niet'. 18,92% gaf aan dat dit tussen 1000 en 4999 euro was, 17,12% stelde dat het niets kostte en 15,32% suggereerde dat deze kostprijs tussen 1 en 999 euro lag.

De vraag werd evenzeer gesteld wie deze kostprijs betaalde. 43,24% antwoordde dat dit de onderneming zelf was. 26,13% beantwoordde deze vraag niet, 12,61% antwoordde dat dit de verzekering was en 11,71% antwoordde 'weet niet'.

Vervolgens werden allerhande mogelijke vormen van schade voorgelegd. Dit leverde de volgende resultaten op.



Figuur 20: In welke mate ondervond uw onderneming schade ten gevolge van het criminaliteitsprobleem? (N=109)

In figuur 20 lezen we af dat de schade die een onderneming ondervond ten gevolge van het criminele feit op veel vlakken verwaarloosbaar was. 27,53% van de bevraagden stelde dat de schade 'ernstig tot erg' was op financieel vlak, 23,85% antwoordde 'ernstig tot erg' op materieel vlak en 21,10% gaf aan dat ze 'ernstige tot erge' schade ondervonden bij interne operationele activiteiten.

Sommige respondenten suggereren een andere vorm van schade, zoals emotionele schade ten gevolge van bedreiging, schade aan de omheining, het stilvallen van enkele belangrijke projecten, een geforceerde toegangsdeur, …

Aan het einde van de vragenlijst werden nog enkele vragen gesteld aangaande de aandacht en de opvolging die men besteedde aan het slachtofferschap.

	Ja	Nee	Weet niet/geen antwoord
Er is een organisatie die ondernemingen helpt en ondersteunt indien zij criminaliteit meemaken	38,40%	22,40%	39,20%
We deden reeds een beroep op een organisatie die ondernemingen helpt en ondersteunt indien zij criminaliteit meemaken	20,80%	65,60%	13,60%
Er zijn psychosociale opvangmogelijkheden waarbij onze medewerkers terechtkunnen indien zij criminaliteit meemaken	66,40%	15,20%	18,40%
We vinden dat er voldoende opvangmogelijkheid is binnen onze onderneming indien iemand criminaliteit meemaakt	52%	26,40%	21,60%
Er is een vertrouwenspersoon voor deze materie in onze onderneming	65,60%	24,80%	9,60%
Er is een anoniem meldpunt in onze onderneming	45,60%	45,60%	8,80%
Er is een procedure in onze onderneming voor het melden van verdachte handelingen op/naast de werkvloer?	54,40%	36,80%	8,80%
Er is een extern aanspreekpunt (slachtofferhulp, idewe) in dit domein	56,80%	30,40%	12,80%
Er is een intern aanspreekpunt (bedrijfspsychologe, arts) in dit domein	40,80%	45,60%	13,60%

Tabel 6: Duid aan of u akkoord gaat met de volgende stellingen: (N=125)

66,4% antwoordde 'ja' op de vraag of er psychosociale opvangmogelijkheden zijn waar medewerkers terechtkunnen indien zij criminaliteit meemaken. Een gelijkaardig percentage (namelijk 65,6%) beaamde dat er een vertrouwenspersoon voor deze materie is in de onderneming. Iets meer dan de helft van de respondenten (56,8%) duidde aan dat er een extern aanspreekpunt (slachtofferhulp, idewe) in dit domein is en 54,4% gaf aan dat er een procedure is in de onderneming voor het melden van verdachte handelingen op/naast de werkvloer. De helft van de respondenten stelde dat er voldoende opvangmogelijkheden zijn binnen de onderneming indien iemand criminaliteit meemaakt. Tot slot gaf 65,6% aan dat zij nog geen beroep deed op een organisatie die ondernemingen helpt en ondersteunt indien zij criminaliteit meemaken.

We vonden enkele statistisch significante verbanden (matig of redelijk) indien we deze stellingen kruisten met de achtergrondvraag naar het aantal medewerkers in de onderneming:

- Bij de eerste twee stellingen, omtrent het bestaan van en beroep doen op organisaties die ondernemingen helpen wanneer zij te maken krijgen met criminaliteit, zien we dat de kleine ondernemingen vaker 'nee' antwoordden.
- De vraag naar psychosociale opvangmogelijkheden werd vooral door grote bedrijven positief beantwoord.
- 'Voldoende opvangmogelijkheid binnen de onderneming indien iemand criminaliteit meemaakt': hoe groter de onderneming, hoe positiever men antwoordde.
- 'Er is een vertrouwenspersoon voor deze materie in onze onderneming' en 'Er is een anoniem meldpunt in onze onderneming': de ondernemingen die tot 50 medewerkers tewerkstellen, antwoordden vaker nee.
- 'Er is een procedure in onze onderneming voor het melden van verdachte handelingen op/naast de werkvloer': ondernemingen met meer dan 251 medewerkers antwoordden over het algemeen positiever.
- 'Er is een extern aanspreekpunt': ondernemingen met meer dan 51 medewerkers antwoordden positiever.
- 'Er is een intern aanspreekpunt': ondernemingen met meer dan 1001 medewerkers antwoordden positiever.

4. Beschouwingen van de interactieve werksessie

In een interactieve werksessie (IW) werden de onderzoeksresultaten van deze barometer besproken met de partnerorganisaties. In wat volgt behandelen we enkele beschouwingen die uit deze sessie naar voren kwamen.

4.1 Werkgever versus werknemer

De stellingen uit de eerste tabel wezen onder meer op het feit dat werknemers minder aandacht zouden besteden aan beveiliging in een onderneming dan werkgevers. Wanneer dit resultaat werd besproken in de IW, werd gesteld dat zowel werkgevers als medewerkers een cruciale rol hebben in de beveiliging van de onderneming. Het hoge percentage respondenten dat het eens was met de stelling 'Onze directie besteedt aandacht aan beveiliging', kan mogelijk verklaard worden doordat veel leidinggevenden deze vragenlijst invulden, en het leidinggevend kader zichzelf verantwoordelijk acht voor de beveiliging in de onderneming. "*De veiligheid op het hoogste niveau staat hoger op de agenda*", aldus een deelnemer. Ten slotte voegde iemand hier aan toe dat de preventieve boodschappen op het domein van beveiliging misschien niet altijd doorsijpelen.

Ook gaf ongeveer 30% van de respondenten aan niet akkoord te gaan met de stelling dat er in de onderneming bewustmakingsactiviteiten worden georganiseerd in het kader van beveiliging. In de interactieve werksessie werd aangegeven dat deze resultaten in lijn liggen met de cijfers bij de stelling 'onze medewerkers besteden aandacht aan beveiliging'. Medewerkers worden minder bewust gemaakt van beveiliging in de onderneming, wat resulteert in een verminderde aandacht hieraan. Bovendien ontbreekt het vaak aan tijd om de mensen voldoende bewust te maken, aldus een deelnemer: "*In veel van onze sectoren ligt de werkdruk hoog en er is geen tijd om dit soort van activiteiten te organiseren*". Het is niettemin belangrijk dat hier tijd voor vrijgemaakt wordt.

Een opvallende bevinding is dat ongeveer 47,34% stelde dat er weinig of geen tests of controles op het vlak van beveiliging worden georganiseerd in de onderneming, wat als problematisch werd gepercipieerd in de IW.

Tot slot is het niet onbelangrijk om te vermelden dat sommige ondernemingen nauwgezet omgaan met de communicatie inzake beveiliging. Hierdoor wordt deze informatie niet altijd prijsgegeven.

4.2 Cybercriminaliteit als risico

De feiten waarvan men wel denkt slachtoffer te kunnen worden, leken voor de deelnemers aan de IW aannemelijk. Cybercriminaliteit is een reëel risico en men is zich hiervan bewust. Anderzijds werd gesteld dat het problematisch kan zijn dat twee derde van de respondenten dit niet als een risico inschat, wetende dat cybercrime zo sterk in opmars is. Eén organisatie haalde aan dat bepaalde sectoren meer met cybercriminaliteit te maken krijgen dan andere. Zo is ICT-criminaliteit weinig gekend in de landbouw, bosbouw en visserij.

Het feit dat geweld en agressie frequent naar voren treden als risico werd beaamd, in het bijzonder door een deelnemer die de menselijke gezondheidszorg en maatschappelijke dienstverlening vertegenwoordigt. Ambulanciers, onthaalmedewerkers aan spoeddiensten, verzorgers in rusthuizen, verplegend personeel in ziekenhuizen en/of psychiatrische instellingen, … krijgen vaak met agressie en geweld te maken. Deze agressie wordt soms ook gepleegd door de patiënt. Bovendien zijn ziekenhuizen, rusthuizen en instellingen doorgaans publiekelijk toegankelijke plaatsen waardoor zij frequent worden blootgesteld aan het publiek en aldus meer risico lopen om slachtoffer te worden van een bepaalde vorm van bedreiging, geweld en agressie.

In de interactieve werksessie werd de lagere algemene risico-inschatting als een 'logisch' onderzoeksresultaat beschouwd. Kleine ondernemingen percipiëren criminaliteitsvormen als mensenhandel, mensensmokkel of witwassen als een ver-van-mijn-bed show, en denken er dus ook geen slachtoffer van te worden.

4.3 Veiligheidscultuur, het management en het beleid inzake beveiliging in uw onderneming

Op de vraag of men zicht heeft op de wijzigingen van wettelijke voorschriften en bepalingen inzake beveiliging in ondernemingen, antwoordde 68,94% 'ja' en 31,06% 'nee'. Daarnaast stelde 56,6% van de bevraagden dat er een beleid is om zich te beveiligen tegen criminaliteit in de onderneming en 43,4% gaf aan dat dit niet het geval is. Meerdere respondenten die werken in een kleine onderneming antwoordden 'nee' op de vraag of er in hun onderneming een beleid is om zich te beveiligen tegen criminaliteit. Dit verband werd gecontextualiseerd in de IW: "*Als er maar 5 personen werken in een onderneming dan zal zo een veiligheidsbeleid niet direct geformaliseerd worden, maar betreft het eerder een mondelinge overeenkomst of worden bepaalde afspraken tussen personen gemaakt*". Een deelnemer van de IW gaf aan dat dit niet per se betekent dat kleine ondernemingen kwetsbaarder zijn: "*Ze zijn kleiner en ze hebben misschien minder nood aan het beveiligen van zaken, een beleid inzake beveiliging of een specifieke functie die bezig is met beveiliging.*"

67,3% van de ondernemingen gaven aan maatregelen te treffen in de strijd tegen criminaliteit. Van de ondernemingen die 'ja' antwoordden, vond 75% dit gepaste of juiste maatregelen. In de IW werden deze resultaten verklaard door het gegeven dat de hoofdmoot van de bevraagden leidinggevenden zijn die de maatregelen zelf ontwikkelen en uitvoeren, en ze aldus als 'gepaste' maatregelen beschouwen.

De hoofredenen om als onderneming te investeren in veiligheid zijn (cfr. figuur 4):

1. Het beschermen van personen
2. Het beschermen van de infrastructuur
3. Het beschermen van de informatie
4. Het beschermen van het product of de dienst

Het beschermen van het imago komt summier aan bod. In de IW werd dit aangehaald als een opvallend resultaat. Men stelde dat dit percentage heel laag is in een tijd waarin media en publiciteit een centrale rol spelen. De respondenten maakten wellicht een onderscheid tussen primaire en secundaire redenen, waarbij de primaire redenen eerder het beschermen van personen, infrastructuur, informatie, producten of diensten betreffen, en er pas in tweede instantie aan het imago gedacht wordt. Een deelnemer vond het beschermen van personen logisch omwille van de finaliteit van zijn sector, namelijk menselijke gezondheidszorg en maatschappelijke dienstverlening. In de IW stelde een betrokken partner: "*Het is goed dat men eerder denkt aan personen en informatie en pas in laatste instantie aan het imago*".

De belangrijkste verantwoordelijke voor de veiligheid in de onderneming is de werkgever, aldus de respondenten. In de IW werd verduidelijkt dat dit in lijn ligt met de resultaten van de eerste stellingen (tabel 1), en aantoont dat de werknemer opnieuw van ondergeschikt belang is. De functie van de persoon die de vragenlijst invult, is evenzeer belangrijk: is dit een directeur of een arbeider? Uit de achtergrondvragen bleek dat dit in grote mate leidinggevende functies zijn.

Een deelnemer gaf aan dat de overheid een belangrijke rol heeft: "*De overheid heeft een belangrijke rol in het hele veiligheidsverhaal, zij moet voldoende aandacht besteden aan veiligheid en daar ook middelen aan spenderen opdat dit doorvloeit naar de organisatie, de werkgever en de werknemers*". Wat betreft de politie, werd gesteld dat er frequent wordt samengewerkt met de politie.

"*Dat de private veiligheid pas op de zesde plaats staat is niet zo verwonderlijk,*" aldus een deelnemer aan de IW, "*de private sector wordt altijd gezien als de junior partner, dit is de mentaliteit die er heerst*".

4.4 IT-beveiliging

93,94% van de bevraagden gaf aan dat IT-beveiliging belangrijk is in een onderneming. In de interactieve werksessie werd aangegeven dat de kleine ondernemingen kwetsbaarder naar voren komen. De reden waarom IT-beveiliging minder aan bod komt in kleinere ondernemingen werd verklaard door:

- Gebrek aan tijd
- Gebrek aan kennis
- De leeftijd: de generatie kan een rol spelen in het besteden van aandacht aan IT-beveiliging.

Tijdens de IW werd het hoge percentage respondenten dat stelt dat de organisatie regelmatig back-ups maakt verklaard doordat de meeste systemen automatisch back-ups nemen. De deelnemers aan de IW reageerden verontwaardigd dat 30% van de respondenten aangaf dat er niet gesensibiliseerd wordt. Dit ligt weliswaar in lijn met de antwoorden op eerdere stellingen, waarbij aangegeven werd dat er slechts beperkt aan sensibilisering wordt gedaan. Het is echter wel cruciaal dat deze 10 maatregelen bij alle werknemers worden toegepast en dus ook de werknemer geresponsabiliseerd wordt in dit verhaal. In de IW werd gesteld dat er een duidelijk onderscheid moet gemaakt worden tussen grote en kleine ondernemingen inzake IT-beveiliging.

Tot slot gaf een deelnemer aan dat de GDPR-wetgeving een reden kan zijn waarom meerdere ondernemingen bezig zijn met IT-beveiliging.

4.5 Fysieke en organisatorische beveiliging

De vormen van fysieke en organisatorische beveiliging werden besproken in de IW, waarbij werd aangegeven dat de meest voorkomende vormen van beveiliging ook degene zijn die het best te implementeren zijn. Het kan echter ook zijn dat deze vormen eenvoudig te manipuleren zijn. In die zin zou er meer moeten geïnvesteerd worden in moeilijker te manipuleren beveiliging, of kan er geopteerd worden voor een combinatie van meerdere technieken. Het belang van sensibiliseren en het betrekken van alle medewerkers in de beveiliging werd nogmaals onderstreept.

Ook de cijfers over de pre-employment screening werden besproken in de IW. Zo werd aangegeven dat dergelijke screenings verplicht zijn in bepaalde sectoren, om bijvoorbeeld een vergunning te krijgen, en soms heeft men een bewijs van goed gedrag en zeden nodig om aan de slag te kunnen gaan. Private werkgevers hebben echter niet altijd toegang tot allerhande databanken. De intensiteit van de screening wordt evenzeer aangehaald: gaat het over een soort van nieuwsgierigheid vanuit de werkgever of betreft het een doorgedreven screening? Enkele deelnemers aan de IW stelden dat dergelijke screenings vaak geoutsourcet worden aan een privaat bureau.

Het percentage in-employment screening werd beschouwd als een logisch gevolg: "*Als men aan pre-employmentscreening doet, doet men ook aan in-employmentscreening".* Werknemerscriminaliteit zoals diefstal door het eigen personeel is een reëel probleem, dus is het logisch dat dergelijke screenings gebeuren.

4.6 Slachtofferschap

4.6.1 **Ondernemingen werden de laatste 12 maanden het vaakst slachtoffer van cybercriminaliteit**

De deelnemers aan de IW percipieerden het percentage slachtofferschap van 'beschadiging' als hoog. Een mogelijke verklaring die aan bod kwam was dat in grote bedrijven vormen van beschadiging vaker aangegeven moeten worden. De kans op rapportage is groter in grote bedrijven, ook omdat er bijvoorbeeld met bedrijfsvoertuigen gewerkt wordt.

Aangaande het slachtofferschap van 'agressie en geweld' werden zowel internen (eigen personeel) als externen (anderen) aangeduid als daders. Ook de grootte van het bedrijf zorgt ervoor dat er meer feiten voorkomen: "*Hoe groter het bedrijf, hoe groter de kans op onderlinge conflicten*".

Er werd tijdens de IW een verschil gemaakt tussen de delicten 'beschadiging' en 'agressie, geweld': beschadiging kan onbewust gebeuren (bijvoorbeeld iemand die tegen een paaltje of tegen een auto rijdt zonder dat hij het opmerkt) terwijl geweld en agressie bewuste handelingen zijn die gesteld worden door de dader. In die zin werd dit hoge percentage als problematischer beschouwd.

Het hoge percentage van agressie en geweld werd door de vertegenwoordiger van de sector menselijke gezondheidszorg en maatschappelijke dienstverlening beaamd. In deze sector wordt men vaak met dergelijke criminaliteitsvormen geconfronteerd. Enerzijds situeren zich in deze sector veel publiek toegankelijke plaatsen waardoor zij frequent worden blootgesteld aan geweld, agressie, beschadiging en ongeoorloofde toegang door externen. Anderzijds werd er gewag gemaakt van geweld en agressie gepleegd door patiënten (cfr. ziekenhuizen, rusthuizen, psychiatrische instellingen, thuisverpleging, thuishulp, andere organisaties in de zorgsector…).

Het percentage slachtofferschap van IT-criminaliteit werd evenzeer als hoog gepercipieerd. Als de 'illegale toegang tot IT-systemen' samengenomen werd met 'tussenkomst in data of systemen', merken we dat één

op de drie bevraagden hier slachtoffer van werd in de laatste 12 maanden. Deze cijfers tonen bovendien geen poging meer aan, maar effectieve toegang: "*Men weet dat dit effectief gebeurde in het bedrijf*".

Het hoge percentage slachtofferschap werd door een deelnemer aan de IW verklaard doordat het voornamelijk die ondernemingen zijn die in het verleden slachtoffer werden, die dergelijke enquêtes invullen: "*Zo'n barometers zullen sneller ingevuld worden door mensen die zich betrokken of aangetrokken voelen door deze problematiek*".

In de IW werden de percentages mensensmokkel en -handel als laag gepercipieerd, hoewel er toch behoorlijk wat cases waren de laatste jaren/maanden. Dit kunnen we mogelijk verklaren doordat voornamelijk internationale zaken onder de aandacht kwamen, die enkel betrekking hebben op activiteiten in het buitenland en niet in België.

Mogelijke interpretatieverschillen werden aangehaald bij de beschadiging van voertuigen. Zo werd de vraag gesteld of we eveneens van beschadiging kunnen spreken als dit in het kader van het verkeer (bv. ongeval) gebeurde.

In de IW werd de definitie van het 'ingrijpende' karakter van criminele feiten aangehaald: "*Is dit ingrijpend voor de onderneming of voor de respondent die de barometer invult?".* Het kwantificeren van feiten is hierbij belangrijk: "*Hoe meer persoonlijke gevallen, hoe ingrijpender dit is voor de onderneming*".

Ook met betrekking tot het aantal gevallen van ongeoorloofde toegang kwamen tijdens de IW vragen naar boven: gebeurt het systematisch dat mensen zich op een ongeoorloofde manier toegang verschaffen tot het bedrijf, is het georganiseerd of betreft het eerder een toevallige verdwaling? Ten slotte werd ook de impact van cybercriminaliteit als een opvallend, doch niet onlogisch, cijfer beschouwd.

4.6.2 Een derde doet geen aangifte bij de politie

De aangiftebereidheid van ondernemingen werd evenzeer aangehaald. Het vermijden van feiten in de toekomst is de primaire reden voor aangifte, en het aangeven van feiten heeft daarnaast ook een belangrijk symbolisch karakter, zoals bij agressie en geweld: "*Wij geven aan om te tonen aan het slachtoffer dat we dit feit ernstig nemen*". Meerdere deelnemers van de IW linken de aangiftecijfers aan de verzekering: enkel als er een aangifte gebeurt, komt de verzekering tussen.

Uit de barometer blijkt dat ongeveer 30% geen aangifte deed bij de politie. Tijdens de interactieve werksessie werd gesuggereerd dat de aangifte gebeurt bij andere sectoren, zoals de private sector. Er spelen ook andere factoren een rol waarom slachtoffers niet aangeven: het zorgt voor een bijkomende administratieve werklast, de zaak wordt intern opgelost of indien de patiënt de dader is, wordt deze misschien niet altijd als dader beschouwd. De relatie patiënt-verzorgende kan een verklarende factor zijn om bepaalde feiten niet aan te geven. Sommige verzorgenden beschouwen dit als een deel van hun job (cfr. psychiatrische instelling, afdeling dementie in het rusthuis…) waarin de persoonlijke beleving van de verzorgende een grote rol speelt: werd ik slachtoffer of niet van bedreiging, geweld, agressie? De sector van menselijke gezondheidszorg en maatschappelijke dienstverlening kan beschouwd worden als een sector waarin dienstverleners aan heel wat kwetsbaarheden worden blootgesteld. Dit vereist extra aandacht.

Daarnaast werd aangehaald dat het belangrijk is om een zicht te krijgen op de feiten en vervolgens de link te leggen met het al dan niet aangeven van deze feiten. Tevens werd gesteld dat de aangiftebereidheid moet gestimuleerd en vereenvoudigd worden, want er wordt op politioneel niveau te weinig aandacht besteed aan ondernemingscriminaliteit.

Een deelnemer aan de IW stelt dat de aangifte-resultaten per feit moeten bekeken worden: "*Is het zo dat geweld en agressie meer worden aangegeven dan ladingdiefstal?"*

4.6.3 Eigenschappen van het crimineel feit

De vraag werd gesteld wat het verdere gevolg was van het proces-verbaal van het 'meest ingrijpende' feit. 38,57% stelde dat de zaak nog in behandeling was en 30% gaf aan dit niet te weten. Het percentage 'nog in behandeling' werd in de IW als een logisch resultaat beschouwd, omdat er in deze barometer werd gepeild naar feiten die de laatste 12 maanden gebeurden. Sommigen antwoordden 'ik weet het niet', wat eveneens kan wijzen op het feit dat de zaak nog in behandeling is en men het gevolg nog niet weet. Het antwoord 'ik weet het niet' werd in de context van grote ondernemingen ook als vanzelfsprekend beschouwd, omdat men hier niet altijd van op de hoogte wordt gebracht. Het percentage veroordelingen werd als laag beschouwd en bevestigt volgens sommigen het stereotiep van de straffeloosheid: "*Het klopt dus wat mensen denken*".

Tot slot kwam de schade in de IW aan bod, waarbij gewezen werd op het feit dat de mentale schade groot kan zijn maar dit niet altijd goed uit te drukken valt. De invloed op de operationele activiteit kan groot zijn omdat werknemers werkonbekwaam kunnen worden. Daarnaast kan er schade zijn op een indirect niveau, waardoor er opnieuw iemand aangenomen moet worden.

5. Enkele kritische beschouwingen en aanbevelingen

In dit rapport worden enkele trends weergegeven over de beveiliging in ondernemingen. De barometer genereert bovendien cijfermatige gegevens over de risico-inschatting en het slachtofferschap van ondernemingen. Deze barometer laat toe om bepaalde veronderstellingen te objectiveren.

Het gegeven dat velen bezig zijn met beveiliging, ook in KMO's, wordt als een positieve trend beschouwd. Niettemin blijken nog veel ondernemingen onvoldoende voorbereid op criminaliteit: er is een gebrek aan beleid of er worden geen maatregelen getroffen, er worden weinig tests of controles uitgevoerd, men heeft het gevoel dat men onvoldoende voorbereid is op eventuele veiligheidsincidenten… In dit kader worden er enkele kritische beschouwingen en aanbevelingen geformuleerd. We eindigen met het opsommen van een 20-puntenprogramma.

Vooreerst wordt gewezen op ieders verantwoordelijkheid: iedereen is verantwoordelijk voor de veiligheid in de onderneming. De verantwoordelijkheid van de veiligheid is dus een taak van zowel werkgever als werknemer.

Cybercriminaliteit is en blijft een belangrijk topic. Het werd in de barometer niet alleen als een belangrijk risico gepercipieerd, maar liefst 42,6% van de ondernemingen werd de laatste 12 maanden ook effectief slachtoffer van één van de vijf bevraagde vormen van cybercriminaliteit. Er dient dan ook meer aandacht besteed te worden aan het sensibiliseren en voorkomen ervan. Kleine ondernemingen dienen bovendien extra aandacht te besteden aan deze vorm van criminaliteit. Vuistregels - zoals het tijdig veranderen van paswoorden - moeten meer meegedeeld worden. Als vastgesteld wordt dat één derde de laatste 12 maanden slachtoffer werd van phishing, is het cruciaal dat men als onderneming kort op de bal speelt en zijn preventiecampagnes hierop ent.

Naast cybercriminaliteit duiken ook beschadiging van een voertuig of eigendom en geweld en agressie op als feiten waar ongeveer 40% van de bevraagde ondernemingen slachtoffer van werd de laatste 12 maanden. Dergelijke feiten kunnen een bijzonder grote impact hebben op een onderneming of een werknemer in de onderneming. Geweldsdelicten en agressie worden als meest ingrijpend beschouwd: dit kan erg ingrijpend zijn op persoonlijk niveau, maar hoeft niet noodzakelijk een grote impact te hebben op de onderneming. Niettemin dient hier aandacht aan besteed te worden, door middel van de creatie van een meldpunt in de onderneming, het erkennen van slachtoffers en het aanbieden van hulp bij slachtofferschap, het stimuleren en begeleiden van de aangifte…

Ongeveer een kwart van de ondernemingen dat slachtoffer werd, gaf dit niet aan bij de politie. Redenen zoals 'omdat dit toch geen resultaat oplevert', 'omdat men er toch niks kan aan doen' en 'omdat we de dader kennen' komen aan bod. De aangiftebereidheid dient gestimuleerd te worden. Een extra investering in het geven van advies over wat er kan aangegeven worden en wat niet, hoe men iets kan aangeven en waar men dit best aangeeft dringt zich op.

Een adequaat veiligheidsbeleid en een goede beveiliging in een onderneming hebben een belangrijke externe en interne functie. Het toont aan de buitenwereld hoe men als onderneming op een professionele manier omgaat met potentiële bedreigende factoren. Het toont bovendien aan dat men als onderneming zijn maatschappelijke verantwoordelijkheid opneemt. Het beschermt en verbetert het imago en stimuleert personeel om langer te blijven werken voor de onderneming (Europees Agentschap voor veiligheid en gezondheid op het werk, 2008). Dit is een belangrijk gegeven in een maatschappij waar 'job hopping' aan belang wint (LiveCareer, 2018).

Er worden tot slot tips opgesomd om zich als bedrijf te beveiligen (o.a. Tolsma, 2011; Korthals Altes & Armstrong, 2017; FOD Economie, 2017).

Voorkomen is beter dan genezen…

1. Iedereen (zowel werkgever als werknemer) is verantwoordelijk voor veiligheid.
2. Maak iedereen in de onderneming bewust van de gevaren en beveiligingsprocedures. Veel incidenten kunnen vermeden worden als men weet hoe op een veilige manier om te gaan met informatie.
3. Stel een deskundige aan: een persoon die intern verantwoordelijk is voor de veiligheid in het bedrijf en dit continu bewaakt.
4. Identificeer en beveilig belangrijke informatie.
5. Geef slechts een beperkte groep mensen toegang tot de bedrijfsgeheimen.
6. Scherm de toegang tot bedrijfskritische plaatsen en gegevens af.
7. Ten aanzien van leveranciers en belangrijke afnemers kunnen veiligheidseisen worden gesteld.
8. Zorg naast een goede cybersecurity ook voor fysieke beveiliging.
9. Gebruik professionele en moderne netwerkapparatuur.
10. Hou de software up-to-date.
11. Kies sterke wachtwoorden.
12. Het beheren van toegang tot de computers is belangrijk, geef slechts een paar IT-specialisten toegang.
13. Investeer in opleidingen, trainingen, sensibilisatiecampagnes in IT-beveiliging.
14. Surf veilig op het internet.
15. Vertrouw niet blindelings op opslagdiensten waar de gegevens worden opgeslagen of verzonden, zoals Dropbox of WeTransfer.
16. Back-ups maken is cruciaal, zo vermijdt men het verlies van bepaalde applicaties of programma's.
17. Denk ook aan de gevaren buiten het bedrijfsnetwerk, zoals usb-sticks, usb-portals, tablets, smartphones en laptops. Beveilig dus mobiele apparaten.

Als men slachtoffer werd…

18. Zorg voor een professionele interne begeleiding van het slachtoffer.
19. Neem het slachtoffer serieus, wees een luisterend oor en vermijdt secundaire victimisatie.
20. Geef dit aan bij de politie.

6. Bibliografie

Algemeen Dagblad (2019). *Weinig zicht op slachtoffers van mensenhandel en uitbuiting.* Retrieved from https://www.ad.nl/binnenland/rapport-weinig-zicht-op-slachtoffers-van-mensenhandel-en-uitbuiting~a5e40067/

Allianz Risk Barometer (2018). Retrieved from https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2018.html [Mei 2018]

Bafort, T. (2016). *Screening van werknemers*. Retrieved from https://lib.ugent.be/fulltxt/RUG01/002/304/239/RUG01-002304239_2016_0001_AC.pdf [Maart 2019]

Belga (2016). *Banden tussen drugshandel en terrorisme worden steeds sterker*. Retrieved from https://www.hln.be/nieuws/buitenland/banden-tussen-drugshandel-en-terrorisme-worden-steeds-sterker~a76e99d2/ [Maart 2019]

Belga (2018). *België en Nederland vormen één drugsmarkt: dus nood aan één aanpak*. Retrieved from https://www.hln.be/nieuws/binnenland/-belgie-en-nederland-vormen-een-drugsmarkt-dus-nood-aan-een-aanpak~a0445397/ [Maart 2019]

Cybersecurity strategy research: Common tactics, issues with implementation, and effectiveness. Tech Pro Research. Retrieved from http://www.techproresearch.com/downloads/cybersecurity-strategy-research-common-tactics-issues-with-implementation-and-effectiveness/ [April 2018]

De Tijd (2018). *Ruim derde van bedrijfsfraude gepleegd door eigen personeel*. Retrieved from https://www.tijd.be/ondernemen/algemeen/ruim-derde-van-bedrijfsfraude-gepleegd-door-eigen-personeel/10068628.html [Maart 2019]

Europees Agentschap voor veiligheid en gezondheid op het werk (2008). *De voordelen van goede veiligheid en gezondheid op het werk voor bedrijven*. Retrieved from https://osha.europa.eu/sites/default/files/publications/documents/nl/publications/factsheets/77/Factsheet_77_-_De_voordelen_van_goede_veiligheid_en_gezondheid_op_het_werk_voor_bedrijven.pdf [Maart 2019]

Europees Parlement (2018). *Terrorisme in de EU : terreuraanslagen, sterfgevallen en arrestaties*. Retrieved from http://www.europarl.europa.eu/news/nl/headlines/security/20180703STO07125/terrorisme-in-de-eu-terreuraanslagen-sterfgevallen-en-arrestaties [Maart 2019]

Federale overheidsdienst (2017). *Maak uw bedrijf cyberveilig in 10 stappen*. Retrieved from https://news.economie.fgov.be/163055-een-cyberveilig-bedrijf-in-10-stappen [April 2018]

Federale Politie (2018). *Tendensen 2016-2017. Politiële criminaliteitsstatistieken*. http://www.stat.policefederale.be/assets/pdf/notas/tendensen_2016_2017_PCS.pdf [Oktober 2018]

Guinevere, J. (2010). *Een kwantitatieve analyse van werknemerscriminaliteit in de bedrijfswereld*. Retrieved from https://lib.ugent.be/nl/catalog/rug01:002049471 [Maart 2019]

Hoeffnagel, W. (2016). *Inzetten op IT-beveiliging is nodig om boetes en reputatieschade te voorkomen*. https://dutchitchannel.nl/546429/managers-vinden-it-afdeling-verantwoordelijk-voor-it-beveiliging.html [Maart 2019]

ICT Security in enterprises. Eurostat: Security policy: risks addressed and staff awareness. Retrieved from http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises^ [April 2018]

Korthals Altes, J. & Armstrong, T (2017). *Tien tips om je onderneming beter te beveiligen tegen cybercriminaliteit*. Retrieved from https://mkbgroeit.nl/10-tips-om-onderneming-beter-beveiligen-cybercriminaliteit/ [Maart 2019]

LiveCareer (2018). *Job hopping analysis: trends by generation & education level.* Retrieved from https://www.livecareer.com/wp-content/uploads/2018/05/2018-Job-Hopping-Report.pdf [Maart 2019]

Smets, L., De Kinder, J., & Moor, L. G. (2011). *Proces-verbaal, aangifte en forensisch onderzoek*. Cahiers Politiestudies, 4, Nr. 21.

Techzine (2018). *Middelgrote bedrijven moeten anticiperen op toenemende risico's Industrie 4.0*. Retrieved from https://www.techzine.be/blogs/22957/middelgrote-bedrijven-moeten-anticiperen-op-toenemende-risicos-industrie-4-0.html [Maart 2019]

Tolsma, J. (2011). *Aangiftebereidheid: Welke overwegingen spelen een rol bij de beslissing om wel of niet aangifte te doen*. Proces-verbaal, aangifte en forensisch onderzoek. Cahiers Politiestudies, 21, 11-32.

UNIZO (2016).UNIZO KMO cijfers, September 2016.

van Dijk, JJM, Tseloni, A. & Farrell, G. (Eds.) (2012). *The International Crime Drop: New Directions in Research. Basingstoke: Palgrave Macmillan; Farrell: Five tests for a theory on the crime drop*. Crime Science 2013 2:5

Veilige buurt (2017). *Lage aangiftebereidheid in 2017*. Retrieved from https://veiligebuurt-.nl/nieuws/aangiftebereidheid-erg-laag/ [Maart 2019]

Veiligheidsladder. Retrieved from http://www.veiligheidsladder.org/wp-content/uploads/2016/06/Certificatieschema_Veiligheidsladder_4.0-final.pdf) [April 2018]

Veiligheidsklimaat. Retrieved from (https://blog.sbo.nl/veiligheid/de-menselijke-factor-praktijkervaring-met-de-barometer-veiligheidsklimaat/) [April 2018]

Versteegh, P. (2007). *Haaldelicten en brengdelicten*. Secondant, 3, 68-71.

World Economic Forum (2018). *The global risks Report 2018. 13the Edition*.